? logon

```
*** It is now 2009/08/28 19:00:51 ***
 (Dialog time 2009/08/28 18:00:51)

705TEXT1 is set ON as an alias for 15, 16, 160, 148, 621, 275, 634, 47
705TEXT2 is set ON as an alias for 9, 623, 810, 624, 813, 20, 636
705BIBLIT is set ON as an alias for 77, 35, 583, 2, 65, 233, 99
705NEWSBIB is set ON as an alias for 473, 474, 475
SOFTLIT is set ON as an alias for 256, 278
705ADLIT is set ON as an alias for 635, 570, PAPERSMJ, PAPERSEU
HILIGHT set on as ''   ''
DETAIL set off
KWIC is set to 50.
```

? b
610,613,634,810,813,20,583,474,475,35,65,99,256,9,15,16,148,160,275,621,636,624,2,4
76, 635, 570, PAPERSMJ, PAPERSEU, 47,347,348,349

```
>>>          476 does not exist
>>>1 of the specified files is not available
     28aug09 17:01:20 User264751 Session D640.1
          $0.00    0.247 DialUnits File415
     $0.00  Estimated cost File415
     $0.13  INTERNET
     $0.13  Estimated cost this search
     $0.13  Estimated total session cost   0.247 DialUnits


SYSTEM:OS  - DIALOG OneSearch
  File 610:Business Wire 1999-2009/Aug 28
        (c) 2009 Business Wire.
*File 610: File 610 now contains data from 3/99 forward.
Archive data (1986-2/99) is available in File 810.
  File 613:PR Newswire 1999-2009/Aug 28
        (c) 2009 PR Newswire Association Inc
*File 613: File 613 now contains data from 5/99 forward.
Archive data (1987-4/99) is available in File 813.
  File 634:San Jose Mercury  Jun 1985-2009/Aug 25
        (c) 2009 San Jose Mercury News
  File 810:Business Wire 1986-1999/Feb 28
        (c) 1999 Business Wire
  File 813:PR Newswire 1987-1999/Apr 30
        (c) 1999 PR Newswire Association Inc
  File  20:Dialog Global Reporter 1997-2009/Aug 28
        (c) 2009 Dialog
  File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
        (c) 2002 Gale/Cengage
*File 583: This file is no longer updating as of 12-13-2002.
  File 474:New York Times Abs 1969-2009/Aug 28
        (c) 2009 The New York Times
  File 475:Wall Street Journal Abs 1973-2009/Aug 28
        (c) 2009 The New York Times
  File  35:Dissertation Abs Online 1861-2009/Jul
        (c) 2009 ProQuest Info&Learning
  File  65:Inside Conferences 1993-2009/Aug 28
        (c) 2009 BLDSC all rts. reserv.
```

```
   File  99:Wilson Appl. Sci & Tech Abs 1983-2009/Jul
          (c) 2009 The HW Wilson Co.
   File 256:TecTrends 1982-2009/Aug W4
          (c) 2009 Info.Sources Inc. All rights res.
*File 256: Please see HELP NEWS 256 for the latest
information about TecTrends.
   File   9:Business & Industry(R)  Jul/1994-2009/Aug 27
          (c) 2009 Gale/Cengage
   File  15:ABI/Inform(R) 1971-2009/Aug 27
          (c) 2009 ProQuest Info&Learning
   File  16:Gale Group PROMT(R) 1990-2009/Aug 05
          (c) 2009 Gale/Cengage
*File  16: UD/banner does not reflect last processed date
   File 148:Gale Group Trade & Industry DB 1976-2009/Aug 13
          (c) 2009 Gale/Cengage
*File 148: The CURRENT feature is not working in File 148.
See HELP NEWS148.
   File 160:Gale Group PROMT(R) 1972-1989
          (c) 1999 The Gale Group
   File 275:Gale Group Computer DB(TM) 1983-2009/Jul 30
          (c) 2009 Gale/Cengage
   File 621:Gale Group New Prod.Annou.(R) 1985-2009/Jul 22
          (c) 2009 Gale/Cengage
   File 636:Gale Group Newsletter DB(TM) 1987-2009/Aug 05
          (c) 2009 Gale/Cengage
   File 624:McGraw-Hill Publications 1985-2009/Aug 28
          (c) 2009 McGraw-Hill Co. Inc
   File   2:INSPEC 1898-2009/Aug W3
          (c) 2009 The IET
   File 635:Business Dateline(R) 1985-2009/Aug 28
          (c) 2009 ProQuest Info&Learning
   File 570:Gale Group MARS(R) 1984-2009/Aug 05
          (c) 2009 Gale/Cengage
   File 387:The Denver Post 1994-2009/Aug 27
          (c) 2009 Denver Post
   File 471:New York Times Fulltext 1980-2009/Aug 28
          (c) 2009 The New York Times
   File 492:Arizona Repub/Phoenix Gaz 19862002/Jan 06
          (c) 2002 Phoenix Newspapers
*File 492: File 492 is closed (no longer updating).  Use
Newsroom, Files 989 and 990, for current records.
   File 494:St LouisPost-Dispatch 1988-2009/Jun 19
          (c) 2009 St Louis Post-Dispatch
   File 631:Boston Globe 1980-2009/Aug 28
          (c) 2009 Boston Globe
   File 633:Phil.Inquirer 1983-2009/Aug 28
          (c) 2009 Philadelphia Newspapers Inc
   File 638:Newsday/New York Newsday 1987-2009/Aug 28
          (c) 2009 Newsday Inc.
   File 640:San Francisco Chronicle 1988-2009/Aug 23
          (c) 2009 Chronicle Publ. Co.
   File 641:Rocky Mountain News Jun 1989-2009/Jan 16
          (c) 2009 Scripps Howard News
*File 641: This file has ceased updating
   File 702:Miami Herald 1983-2009/Aug 28
          (c) 2009 The Miami Herald Publishing Co.
   File 703:USA Today 1989-2009/Aug 27
```

```
           (c) 2009 USA Today
  File 704:(Portland)The Oregonian 1989-2009/Aug 27
           (c) 2009 The Oregonian
  File 713:Atlanta J/Const. 1989-2009/Mar 08
           (c) 2009 Atlanta Newspapers
  File 714:(Baltimore) The Sun 1990-2009/Aug 23
           (c) 2009 Baltimore Sun
  File 715:Christian Sci.Mon. 1989-2009/Jul 20
           (c) 2009 Christian Science Monitor
  File 725:(Cleveland)Plain Dealer Aug 1991-2009/Aug 27
           (c) 2009 The Plain Dealer
  File 735:St. Petersburg Times 1989- 2009/May 22
           (c) 2009 St. Petersburg Times
  File 477:Irish Times 1999-2009/Aug 28
           (c) 2009 Irish Times
  File 710:Times/Sun.Times(London) Jun 1988-2009/Aug 28
           (c) 2009 Times Newspapers
  File 711:Independent(London) Sep 1988-2006/Dec 12
           (c) 2006 Newspaper Publ. PLC
*File 711: This file does not update.  See NewsRoom for full
daily coverage from many European sources.
  File 756:Daily/Sunday Telegraph 2000-2009/Aug 28
           (c) 2009 Telegraph Group
  File 757:Mirror Publications/Independent Newspapers 2000-2009/Aug 28
           (c) 2009
  File  47:Gale Group Magazine DB(TM) 1959-2009/Aug 17
           (c) 2009 Gale/Cengage
  File 347:JAPIO Dec 1976-2009/Mar(Updated 090708)
           (c) 2009 JPO & JAPIO
  File 348:EUROPEAN PATENTS 1978-200934
           (c) 2009 European Patent Office
  File 349:PCT FULLTEXT 1979-2009/UB=20090820|UT=20090709
           (c) 2009 WIPO/Thomson

       Set  Items  Description
       ---  -----  -----------
```

? s pd<20010213

Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing

Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
>>>One or more prefixes are unsupported
>>> or undefined in one or more files.
Processed 10 of 51 files ...
Processing
Processing
Processing
Processing
Processing
Processed 20 of 51 files ...
Processing
Processing
Processing
Processed 30 of 51 files ...
Processing
Processing
Processed 40 of 51 files ...
Processing
Processing
Processing
Processing
Processed 50 of 51 files ...
Completed processing all files
       S190499905 PD<20010213

? s (secondhand or (second(w)hand))(w)(content)

```
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processed  10 of  51 files ...
Processing
Processed  20 of  51 files ...
Processing
Processed  50 of  51 files ...
Processing
Completed processing all files
           61432  SECONDHAND
         26971319  SECOND
          9263227  HAND
           136052  SECOND(W)HAND
          7505470  CONTENT
      S2       11  (SECONDHAND OR (SECOND(W)HAND))(W)(CONTENT)
```

? s pd=20010214

```
>>>One or more prefixes are unsupported
>>>  or undefined in one or more files.
      S3   33713  PD=20010214
```

? s (s1 or s3) and s2

```
         90499905  S1
            33713  S3
               11  S2
      S4        2  (S1 OR S3) AND S2
```

? t s4/3/all

4/3/1 (Item 1 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)
(c) 2009 ProQuest Info&Learning. All rights reserved.

02168547   73209730
Managing information in the digital age: How the reader is king

McGovern, Gerry
Irish Marketing Review v13n2 pp: 55-60
2000
ISSN: 0790-7362 **Journal Code:** IMV

Word Count: 3289

4/3/2 (Item 1 from file: 710)
DIALOG(R)File 710: Times/Sun.Times(London)

05658289

ALBION ROVERS; BOOKS

Times of London (TL) - Sunday, JanUary 21, 1990
By: Thomas Hinde
 Section: Features
Word Count: 1,044

? t s4/k/all

4/K/1 (Item 1 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)

Text:
```
...from a piece of content, it needs to prepare it specifically for the
Web. If it merely translates content from printed form, it is offering
second-hand content to the reader, which is clearly
unacceptable.

The typical person who reads information on the Web can be described as
a
scan-reader. Their first...
```

4/K/2 (Item 1 from file: 710)
DIALOG(R)File 710: Times/Sun.Times(London)

Text:

```
 ...Webb & Bower/M Joseph Pounds 15.95) as the muzak of book
publishing. There are plenty of similarities: the bland inoffensiveness
of
both products, their second-hand content, their lack
of vitality. But 3m people all over the world have voluntarily paid
money
for the original Edith Holden title, and no doubt millions...
```

? s ((used(w)content)(5n)(redistribute or redistributes or redistribution or redistributing or redistributed)

>>>Unmatched parentheses

? s (used(w)content)(5n)(redistribute or redistributes or redistribution or redistributing or redistributed)

Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processed 10 of 51 files ...
Processing
Processed 40 of 51 files ...
Processed 50 of 51 files ...
Processing
Completed processing all files
        28248675 USED
         7505470 CONTENT
          527462 REDISTRIBUTE
            7945 REDISTRIBUTES
          729074 REDISTRIBUTION
           19182 REDISTRIBUTING
           93384 REDISTRIBUTED
      S5   9 (USED(W)CONTENT)(5N)(REDISTRIBUTE OR REDISTRIBUTES OR
                    REDISTRIBUTION OR REDISTRIBUTING OR REDISTRIBUTED)

>>> Retrying request [1]
? s (used(w)content)(5n)(sale or sales or sold or selling or sellable)

Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing

```
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processed  10 of  51 files ...
Processing
Processing
Processed  20 of  51 files ...
Processing
Processed  40 of  51 files ...
Processing
Processed  50 of  51 files ...
Processing
Completed processing all files
        28248675  USED
         7505470  CONTENT
         9532677  SALE
        24135110  SALES
         9156611  SOLD
         8981519  SELLING
            8100  SELLABLE
     S6       25  (USED(W)CONTENT)(5N)(SALE OR SALES OR SOLD OR SELLING
OR
                  SELLABLE)
```

? s (used(w)content)(5n)(resale or resales or resold or reselling or resellable or reseller or resaler)

```
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processed  10 of  51 files ...
Processed  40 of  51 files ...
Processing
Processing
Processed  50 of  51 files ...
Completed processing all files
        28248675  USED
         7505470  CONTENT
          262689  RESALE
           22848  RESALES
           88137  RESOLD
           72981  RESELLING
             308  RESELLABLE
          498074  RESELLER
```

```
                260  RESALER
        S7        1  (USED(W)CONTENT)(5N)(RESALE OR RESALES OR RESOLD OR
                     RESELLING OR RESELLABLE OR RESELLER OR RESALER)
```

? s (used(w)content)(5n)(redeliver or redelivers or redeliverable or redelivering or redelivered)

Processing

Processing

Processing

Processing

Processing

```
Processing
Processed  10 of  51 files ...
Processing
Processed  50 of  51 files ...
Completed processing all files
        28248675  USED
         7505470  CONTENT
            1396  REDELIVER
             177  REDELIVERS
               2  REDELIVERABLE
             309  REDELIVERING
            1752  REDELIVERED
        S8        0  (USED(W)CONTENT)(5N)(REDELIVER OR REDELIVERS OR
                     REDELIVERABLE OR REDELIVERING OR REDELIVERED)
```

? ds

```
Set      Items    Description
S1    90499905    PD<20010213
S2          11    (SECONDHAND OR (SECOND(W)HAND))(W)(CONTENT)
S3       33713    PD=20010214
S4           2    (S1 OR S3) AND S2
S5           9    (USED(W)CONTENT)(5N)(REDISTRIBUTE OR REDISTRIBUTES OR
REDI-
                  STRIBUTION OR REDISTRIBUTING OR REDISTRIBUTED)
S6          25    (USED(W)CONTENT)(5N)(SALE OR SALES OR SOLD OR SELLING
OR S-
                  ELLABLE)
S7           1    (USED(W)CONTENT)(5N)(RESALE OR RESALES OR RESOLD OR
RESELL-
                  ING OR RESELLABLE OR RESELLER OR RESALER)
S8           0    (USED(W)CONTENT)(5N)(REDELIVER OR REDELIVERS OR
REDELIVERA-
                  BLE OR REDELIVERING OR REDELIVERED)
```

? s (s1 or s3) and (s5 or s6 or s7)

```
        90499905  S1
           33713  S3
               9  S5
              25  S6
               1  S7
        S9        2  (S1 OR S3) AND (S5 OR S6 OR S7)
```

? t s9/k/all

9/K/1 (Item 1 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

Country	Number	Kind	Date
Legal Status Type	Pub. Date	Kind	Text

Language

Fulltext Availability Available Text	Language	Update	Word Count
Total Word Count (Document A)			
Total Word Count (Document B)			
Total Word Count (All Documents)			

Specification: ...of remote resources (e.g. centralized databases, super computers, etc.) while providing a secure means for charging users based on information and/or resources actually **used**.) support both "translations" of VDE electronic agreements elements into modern language printed agreement elements (such as English language agreements) and translations of electronic rights protection...

9/K/2 (Item 2 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

Country	Number	Kind	Date
Legal Status Type	Pub. Date	Kind	Text

Language

Fulltext Availability Available Text	Language	Update	Word Count
Total Word Count (Document A)			
Total Word Count (Document B)			
Total Word Count (All Documents)			

Specification: ...5 mm in length. The resulting granules are dried in a drum dryer; hot (300(degree)C) flue gas introduced in a countercurrent stream is **used as** drying agent.

The contact **period** of the flue gas and the granules is adjusted to about 5 minutes; in this way the surface of the granules cannot reach a temperature...

? s (s1 or s3) and ((content)(2n)(redistribute or redistributes or redistribution or redistributing or redistributed)) and (music or movie or movies or audio or book or books) and (digital or electronic or online or internet or web)

Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processed 10 of 51 files ...
Processing
Processed 20 of 51 files ...
Processing
Processed 40 of 51 files ...
Processing
Completed processing all files
         90499905 S1
            33713 S3
          7505470 CONTENT
           527462 REDISTRIBUTE
             7945 REDISTRIBUTES
           729074 REDISTRIBUTION
            19182 REDISTRIBUTING
            93384 REDISTRIBUTED
             1710 CONTENT(2N)((((REDISTRIBUTE OR REDISTRIBUTES) OR
                   REDISTRIBUTION) OR REDISTRIBUTING) OR REDISTRIBUTED)
          5639748 MUSIC
          2572337 MOVIE
          1523805 MOVIES
          2925444 AUDIO
          7941162 BOOK
          5111975 BOOKS
          7196587 DIGITAL
         10522132 ELECTRONIC
          9430219 ONLINE
         12799271 INTERNET
         19032160 WEB
      S10   195 (S1 OR S3) AND ((CONTENT)(2N)(REDISTRIBUTE OR
                   REDISTRIBUTES OR REDISTRIBUTION OR REDISTRIBUTING OR
                   REDISTRIBUTED)) AND (MUSIC OR MOVIE OR MOVIES OR
AUDIO OR

```
                   BOOK OR BOOKS) AND (DIGITAL OR ELECTRONIC OR ONLINE
OR
                   INTERNET OR WEB)
```

? s (s1 or s3) and ((content)(2n)(resale or resales or resold or reselling or resellable or reseller or resaler)) and (music or movie or movies or audio or book or books) and (digital or electronic or electronically or digitally or online or internet or web)

Processing

Processing

Processing

Processing

Processing

Processing

```
Processing
Processed  10 of  51 files ...
Processing
Processed  20 of  51 files ...
Processing
Processed  50 of  51 files ...
Completed processing all files
         90499905  S1
            33713  S3
          7505470  CONTENT
           262689  RESALE
            22848  RESALES
            88137  RESOLD
            72981  RESELLING
              308  RESELLABLE
           498074  RESELLER
              260  RESALER
              908  CONTENT(2N)((((((RESALE OR RESALES) OR RESOLD) OR
                   RESELLING) OR RESELLABLE) OR RESELLER) OR RESALER)
          5639748  MUSIC
          2572337  MOVIE
          1523805  MOVIES
          2925444  AUDIO
          7941162  BOOK
          5111975  BOOKS
          7196587  DIGITAL
         10522132  ELECTRONIC
           718802  ELECTRONICALLY
           258194  DIGITALLY
          9430219  ONLINE
         12799271  INTERNET
         19032160  WEB
     S11       95  (S1 OR S3) AND ((CONTENT)(2N)(RESALE OR RESALES OR
RESOLD
                   OR RESELLING OR RESELLABLE OR RESELLER OR RESALER))
AND
                   (MUSIC OR MOVIE OR MOVIES OR AUDIO OR BOOK OR BOOKS)
AND
                   (DIGITAL OR ELECTRONIC OR ELECTRONICALLY OR DIGITALLY
OR
                   ONLINE OR INTERNET OR WEB)
```

? s (s1 or s3) and ((content)(2n)(redeliver or redelivers or redeliverable or redelivering or redelivered or redelivery)) and (music or movie or movies or audio or book or books) and (digital or electronic or electronically or digitally or online or internet or web)

Processing

Processing

Processing

```
Processing
Processed  20 of  51 files ...
Completed processing all files
         90499905  S1
            33713  S3
          7505470  CONTENT
             1396  REDELIVER
              177  REDELIVERS
                2  REDELIVERABLE
              309  REDELIVERING
             1752  REDELIVERED
             3733  REDELIVERY
               60  CONTENT(2N)(((((REDELIVER OR REDELIVERS) OR
                   REDELIVERABLE) OR REDELIVERING) OR REDELIVERED) OR
                   REDELIVERY)
          5639748  MUSIC
          2572337  MOVIE
          1523805  MOVIES
          2925444  AUDIO
          7941162  BOOK
          5111975  BOOKS
          7196587  DIGITAL
         10522132  ELECTRONIC
           718802  ELECTRONICALLY
           258194  DIGITALLY
          9430219  ONLINE
         12799271  INTERNET
         19032160  WEB
     S12        10  (S1 OR S3) AND ((CONTENT)(2N)(REDELIVER OR REDELIVERS
OR
                   REDELIVERABLE OR REDELIVERING OR REDELIVERED OR
                   REDELIVERY)) AND (MUSIC OR MOVIE OR MOVIES OR AUDIO
OR
                   BOOK OR BOOKS) AND (DIGITAL OR ELECTRONIC OR
                   ELECTRONICALLY OR DIGITALLY OR ONLINE OR INTERNET OR
WEB)
```

? ds

```
Set      Items   Description
S1   90499905   PD<20010213
S2         11   (SECONDHAND OR (SECOND(W)HAND))(W)(CONTENT)
S3      33713   PD=20010214
S4          2   (S1 OR S3) AND S2
S5          9   (USED(W)CONTENT)(5N)(REDISTRIBUTE OR REDISTRIBUTES OR
REDI-
```

```
            STRIBUTION OR REDISTRIBUTING OR REDISTRIBUTED)
S6        25   (USED(W)CONTENT)(5N)(SALE OR SALES OR SOLD OR SELLING
OR S-
            ELLABLE)
S7         1   (USED(W)CONTENT)(5N)(RESALE OR RESALES OR RESOLD OR
RESELL-
            ING OR RESELLABLE OR RESELLER OR RESALER)
S8         0   (USED(W)CONTENT)(5N)(REDELIVER OR REDELIVERS OR
REDELIVERA-
            BLE OR REDELIVERING OR REDELIVERED)
S9         2   (S1 OR S3) AND (S5 OR S6 OR S7)
S10      195   (S1 OR S3) AND ((CONTENT)(2N)(REDISTRIBUTE OR
REDISTRIBUTES
            OR REDISTRIBUTION OR REDISTRIBUTING OR REDISTRIBUTED))
AND (-
            MUSIC OR MOVIE OR MOVIES OR AUDIO OR BOOK OR BOOKS) AND
(DIGI-
            TAL OR ELECTRONIC OR ONLINE OR INTERNET OR WEB)
S11       95   (S1 OR S3) AND ((CONTENT)(2N)(RESALE OR RESALES OR
RESOLD -
            OR RESELLING OR RESELLABLE OR RESELLER OR RESALER)) AND
(MUSIC
            OR MOVIE OR MOVIES OR AUDIO OR BOOK OR BOOKS) AND
(DIGITAL OR
            ELECTRONIC OR ELECTRONICALLY OR DIGITALLY OR ONLINE OR
INTER-
            NET OR WEB)
S12       10   (S1 OR S3) AND ((CONTENT)(2N)(REDELIVER OR REDELIVERS
OR R-
            EDELIVERABLE OR REDELIVERING OR REDELIVERED OR
REDELIVERY)) A-
            ND (MUSIC OR MOVIE OR MOVIES OR AUDIO OR BOOK OR BOOKS)
AND (-
            DIGITAL OR ELECTRONIC OR ELECTRONICALLY OR DIGITALLY OR
ONLINE
            OR INTERNET OR WEB)
```

? s s10 or s11 or s12

```
            195   S10
             95   S11
             10   S12
   S13      300   S10 OR S11 OR S12
```

? s s13 and (right or rights) and (useage or usages or term or terms) and (license or licenses or licensing or licensed)

Processing
Processing
```
Processing
Processed  20 of  51 files ...
Completed processing all files
            300   S13
      18742267   RIGHT
      10604993   RIGHTS
```

```
      2017  USEAGE
     26594  USAGES
  14011326  TERM
  11678045  TERMS
   3180630  LICENSE
   1395611  LICENSES
   3112855  LICENSING
   2167021  LICENSED
S14     32  S13 AND (RIGHT OR RIGHTS) AND (USEAGE OR USAGES OR
TERM
            OR TERMS) AND (LICENSE OR LICENSES OR LICENSING OR
            LICENSED)
```

? rd

```
>>>Duplicate detection is not supported for File 347.

>>>Duplicate detection is not supported for File 348.

>>>Duplicate detection is not supported for File 349.

>>>Records from unsupported files will be retained in the RD set.
    S15     26  RD  (unique items)
```

? t s15/3/all

15/3/1 (Item 1 from file: 613)
DIALOG(R)File 613: PR Newswire
(c) 2009 PR Newswire Association Inc. All rights reserved.

00507453 20010202SFF030 **(USE FORMAT 7 FOR FULLTEXT)**
**Novell Launches Volera - New Venture Takes Flight Targeting Aggressive Growth
in the Content Networking Market Space**

PR Newswire
Friday , February 2, 2001 08:00 EST
**Journal Code: PR Language: ENGLISH Record Type: FULLTEXT Document
Type: NEWSWIRE**
Word Count: 1,731

15/3/2 (Item 2 from file: 613)
DIALOG(R)File 613: PR Newswire
(c) 2009 PR Newswire Association Inc. All rights reserved.

00274744 20000229SFTU017 **(USE FORMAT 7 FOR FULLTEXT)**
**Massive Media Group And Intertrust Announce Digital Rights Management
Partnership for The Global Entertainment And Advertising Markets**

PR Newswire
Tuesday , February 29, 2000 06:00 EST

Journal Code: PR **Language:** ENGLISH **Record Type:** FULLTEXT **Document Type:** NEWSWIRE
Word Count: 1,822

15/3/3 (Item 1 from file: 20)
DIALOG(R)File 20: Dialog Global Reporter

14955014 **(USE FORMAT 7 OR 9 FOR FULLTEXT)**
NOVELL: Novell launches Volera; New venture takes flight targeting aggressive growth in the content networking market space; Nortel Networks and Accenture sign definitive agreements to take minority equity positions

M2 PRESSWIRE
February 02, 2001
Journal Code: WMPR **Language:** English **Record Type:** FULLTEXT
Word Count: 1702

15/3/4 (Item 2 from file: 20)
DIALOG(R)File 20: Dialog Global Reporter

05061354 **(USE FORMAT 7 OR 9 FOR FULLTEXT)**
Digital Watermarking: The Copyright Crawlers

COMPUTERS TODAY , p 90
April 30, 1999
Journal Code: WCOT **Language:** English **Record Type:** FULLTEXT
Word Count: 1540

15/3/5 (Item 1 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)

02358067   115921677
Being negligent and liable: a challenge for information professionals

Hannabuss, Stuart
Library Management   v21n6 pp: 316-329
2000
ISSN: 0143-5124 **Journal Code:** LBM
Word Count: 9693

15/3/6 (Item 2 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)

02096808   64862363
Salon.com is optimistic despite dot-com downturn

Van Dkye, Geoff
Folio: the Magazine for Magazine Management   v29n15 pp: 16-17
Dec 1, 2000
ISSN: 0046-4333 **Journal Code:** FOL
Word Count: 823

15/3/7 (Item 1 from file: 16)
DIALOG(R)File 16: Gale Group PROMT(R)

08146815   **Supplier Number:** 68025418 **(USE FORMAT 7 FOR FULLTEXT)**

Salon.com Is Optimistic Despite Dot-Com Downturn.(interview with senior vice president Scott Rosenberg)(Brief Article)(Interview)
Dyke, Geoff Van
Folio: the Magazine for Magazine Management , v 29 , n 15 , p 16
Dec 1 , 2000
Language: English   **Record Type:** Fulltext
Article Type: Brief Article; Interview
Document Type: Magazine/Journal ; Trade
Word Count: 869

15/3/8 (Item 2 from file: 16)
DIALOG(R)File 16: Gale Group PROMT(R)

07052886   **Supplier Number:** 58378495 **(USE FORMAT 7 FOR FULLTEXT)**

Using the Web to relieve permissions bottlenecks : Yankee, iCopyright take different tacks to same end.(Yankee Book Peddler)(Company Business and Marketing)
Votsch, Victor; Walter, Mark
The Seybold Report on Internet Publishing , v 3 , n 11 , p NA
July , 1999
Language: English   **Record Type:** Fulltext
Document Type: Newsletter ; Trade
Word Count: 1692

15/3/9 (Item 1 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

0019895673   **Supplier Number:** 69969797 (USE FORMAT 7 OR 9 FOR FULL
TEXT)
**Novell launches Volera; New venture takes flight targeting aggressive growth in the
content networking market space; Nortel Networks and Accenture sign definitive
agreements to take minority equity positions.**

M2 Presswire , NA
Feb 2 , 2001
Language: English
Record Type: Fulltext
Word Count: 1881   **Line Count:** 00165

15/3/10 (Item 2 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

12361278   **Supplier Number:** 62599337 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Making Smart Licensing Decisions.

guenther, kim
Computers in Libraries , 20 , 6 , 58
June , 2000
ISSN: 1041-7915
Language: English
Record Type: Fulltext
Word Count: 2445   **Line Count:** 00207

15/3/11 (Item 1 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

02416312   **Supplier Number:** 62599337 **(Use Format 7 Or 9 For** FULL TEXT)
Making Smart Licensing Decisions.(Industry Trend or Event)

guenther, kim
Computers in Libraries , 20 , 6 , 58
June , 2000
ISSN: 1041-7915
Language: English   **Record Type:** Fulltext
Word Count: 2445   **Line Count:** 00207

15/3/12 (Item 2 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

02168765   **Supplier Number:** 20422316 **(Use Format 7 Or 9 For** FULL TEXT **)**
Positioning your business for the 'E-business' future. (includes related articles on four standard's categories, core graphic communication process, content management terminology, Interspace and global education initiative Digital Roadmaps) (Industry Trend or Event)

Davis, Mills
Seybold Report on Publishing Systems , v27 , n12 , p3(16)
March 9 , 1998
ISSN: 0736-7260
Language: English   **Record Type:** Fulltext
Word Count: 11774   **Line Count:** 01030

15/3/13 (Item 3 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01680408   **Supplier Number:** 15103345 **(Use Format 7 Or 9 For** FULL TEXT **)**
Publishing on the Internet for fun and profit. (includes related articles on TCP/IP Internet communications protocol, the Interpedia public domain encyclopedia project on the Internet, observations on using Internet access software and printed and online resources about setting up Internet businesses)

Dyson, Peter E.
Seybold Report on Desktop Publishing , v8 , n8 , p3(12)
April 4 , 1994
ISSN: 0889-9762
Language: ENGLISH   **Record Type:** FULLTEXT
Word Count: 11544   **Line Count:** 00895

Dialog eLink: Order File History
15/3/14 (Item 1 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

01289339

Digital content distribution using web broadcasting services
Verbreitung digitalen Inhalts unter Benutzung eines Internet-Sendeservices
Distribution de contenu numerique utilisant un service de diffusion de donnees

Patent Assignee:

- **International Business Machines Corporation**; (200128)
  New Orchard Road; Armonk, NY 10504; (US)
  (Applicant designated States: all)

Inventor:

- **Mourad, Magda, c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)
- **Munson, Jonathan P., c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)
- **Pacifici, Giovanni, c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)
- **Tantawy, Ahmed, c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)
- **Youssef, Alaa S., c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)

Legal Representative:

- **Ling, Christopher John (80401)**
  IBM United Kingdom Limited, Intellectual Property Department, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)

	Country	Number	Kind	Date	
Patent	EP	1107137	A2	20010613	(Basic)
	EP	1107137	A3	20040428	
Application	EP	2000310981		20001208	
Priorities	US	457563		19991209	
	US	487417		20000120	

Designated States:
AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LI; LU; MC; NL; PT; SE; TR;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-017/30**Abstract Word Count:** 151
NOTE: 18
NOTE: Figure number on first page: 18

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English

Procedural:　　　　　English

Application:　　　　　English

Fulltext Availability	Available Text	Language	Update	Word Count
CLAIMS A		(English)	200124	1260
SPEC A		(English)	200124	46736
Total Word Count (Document A) 47996				
Total Word Count (Document B) 0				
Total Word Count (All Documents) 47996				

01276898

CONTENTS MANAGEMENT SYSTEM, DEVICE, METHOD, AND PROGRAM STORAGE MEDIUM
INHALTSVERWALTUNGSSYSTEM, VORRICHTUNG, VERFAHREN UND PROGRAMMSPEICHERMEDIUM
SYSTEME, DISPOSITIF, PROCEDE ET SUPPORT DE PROGRAMME POUR LA GESTION DE CONTENUS

Patent Assignee:

- **Sony Corporation**; (214028)
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
  (Applicant designated States: all)

Inventor:

- **ISHIBASHI, Yoshihito, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)

- **OHISHI, Tateo, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **MUTO, Akihiro, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **KITAHARA, Jun, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **SHIRAI, Taizou, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)

Legal Representative:

- **DeVile, Jonathan Mark, Dr. et al (91151)**
  D. Young & Co 21 New Fetter Lane; London EC4A 1DA; (GB)

	Country	Number	Kind	Date	
Patent	EP	1128598	A1	20010829	(Basic)
	WO	200119017		20010315	
Application	EP	2000956997		20000907	
	WO	2000JP6089		20000907	
Priorities	JP	99253660		19990907	
	JP	99253661		19990907	
	JP	99253662		19990907	
	JP	99253663		19990907	
	JP	99260638		19990914	
	JP	99264082		19990917	
	JP	99265866		19990920	

Designated States:
DE; FR; GB;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): H04L-009/32; G06F-015/00; H04N-005/91; G11B-020/10; G10K-015/04; H04N-007/167**Abstract Word Count:** 172
NOTE: 0020
NOTE: Figure number on first page: 0020

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: Japanese

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200135	29406
SPEC A	(English)	200135	83907
Total Word Count (Document A) 113313			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 113313			

01273919

**INFORMATION TRANSMISSION SYSTEM, TRANSMITTER, AND
TRANSMISSION METHOD AS WELL AS INFORMATION RECEPTION
SYSTEM, RECEIVER AND RECEPTION METHOD**
INFORMATIONSUBERTRAGUNGSSYSTEM, SENDER,
UBERTRAGUNGSVERFAHREN, SOWIE INFORM ATIONSEMPFANGSSYSTEM,
EMPFANGER UND EMPFANGSVERFAHREN
SYSTEME DE TRANSMISSION D'INFORMATIONS, EMETTEUR ET
RECEPTEUR, PROCEDE DE TRANSMISSION D'INFORMATIONS, PROCEDE DE
RECEPTION D'INFORMATIONS

Patent Assignee:

* **Sony Corporation**; (214028)
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
  (Applicant designated States: all)

Inventor:

* **ISHIBASHI, Yoshihito, c/o Sony Corporation**
  6-7-35, Kitashinagawa, Shinagawa-ku; Tokyo 141-0001; (JP)
* **OHISHI, Tateo, c/o Sony Corporation**
  6-7-35, Kitashinagawa-ku; Shinagawa-ku, Tokyo 141-0001; (JP)

- **MATSUYAMA, Shinako, c/o Sony Corporation**
  6-7-35, Kitashigawa, Shinagawa-ku; Tokyo 141-0001; (JP)
- **ASANO, Tomoyuki, c/o Sony Corporation**
  7-35, Kitashigawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **MUTO, Akihiro, c/o Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **KITAHARA, Jun, c/o Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)

Legal Representative:

- **Pilch, Adam John Michael et al (50481)**
  D. YOUNG & CO., 21 New Fetter Lane; London EC4A 1DA; (GB)

	Country	Number	Kind	Date	
Patent	EP	1134670	A1	20010919	(Basic)
	WO	200116776		20010308	
Application	EP	2000955022		20000825	
	WO	2000JP5742		20000825	
Priorities	JP	99242294		19990827	
	JP	99242295		19990827	
	JP	99242296		19990827	
	JP	99283326		19990827	

Designated States:
DE; FR; GB;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-015/00; G06F-017/60; H04L-009/08; G10K-015/02**Abstract Word Count:** 214
NOTE: 20
NOTE: Figure number on first page: 20

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English

Procedural: English

Application: Japanese

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200138	14242
SPEC A	(English)	200138	53309
Total Word Count (Document A) 67551			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 67551			

01257209

Method and apparatus for uniquely identifying a customer purchase in an electronic distribution system
Verfahren und Apparat zum eindeutigen Identifizieren eines Kundeneinkaufs in einem elektronischen Auslieferungs-System
Methode et appareil pour l'identification unique d'un achat d'un client dans un systeme de distribution electronique

Patent Assignee:

- **Wistron Corporation**; (7754890)
  21 F, No. 88, Sec. 1 Hsin-Tai-Wu Road Hsi-Chih City; Taipei Hsien 221; (TW)
  (Proprietor designated states: all)

Inventor:

- **Dorak, John J., Jr.,c/o IBM United Kingdom Ltd**
  Intel. Property Law,Hursley Park; Winchester,Hampshire S021 2JN; (GB)

Legal Representative:

- **Schaeberle, Steffen et al (93211)**
  Hoefer & Partner Patentanwalte Pilgersheimer Strasse 20; 81543 Munchen; (DE)

	Country	Number	Kind	Date	
Patent	EP	1085443	A2	20010321	(Basic)
	EP	1085443	A3	20050105	
	EP	1085443	B1	20080827	
Application	EP	2000308024		20000914	
Priorities	US	397419		19990917	

Designated States:
AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LI; LU; MC; NL; PT; SE;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-017/60

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0021/00	A	I	F	B	20060101	20080226	H	EP

Abstract Word Count: 123
NOTE: 18
NOTE: Figure number on first page: 18

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English

Procedural:	English
Application:	English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200112	694
SPEC A	(English)	200112	42226
CLAIMS B	(English)	200835	1047
CLAIMS B	(German)	200835	1107
CLAIMS B	(French)	200835	1243
SPEC B	(English)	200835	43289
Total Word Count (Document A) 42927			
Total Word Count (Document B) 46686			
Total Word Count (All Documents) 89613			

01245941

Secure electronic content distribution on CDS and DVDS
Sichere Verteilung von elektronischem Inhalt auf CDs und DVDs
Distribution securisee d'un contenu electronique sur CDs et DVDs

Patent Assignee:

- **International Business Machines Corporation**; (200129)
  New Orchard Road; Armonk, NY 10504; (US)
  (Proprietor designated states: all)

Inventor:

- **Hurtado, Marco M.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Milsted, Kenneth L.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Gruse, George G.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Downs, Edgar,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Lehman, Christopher T.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Spagna, Richard L.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Lotspiech, Jeffrey B.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)

Legal Representative:

- **Ling, Christopher John (80401)**
  IBM United Kingdom Limited, Intellectual Property Department, Hursley Park;
  Winchester,Hampshire SO21 2JN; (GB)

	Country	Number	Kind	Date	
Patent	EP	1077398	A1	20010221	(Basic)
	EP	1077398	B1	20060920	
Application	EP	2000305655		20000705	
Priorities	US	376102		19990817	

Designated States:
AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LI; LU; MC; NL; PT; SE;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-001/00; H04L-029/06

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0001/00	A	I	F	B	20060101	20001128	H	EP
H04L-0029/06	A	I	L	B	20060101	20001128	H	EP

Abstract Word Count: 211
NOTE: 18
NOTE: Figure number on first page: 18

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English

Procedural: English

Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200108	981
SPEC A	(English)	200108	42868
CLAIMS B	(English)	200638	520
CLAIMS B	(German)	200638	534
CLAIMS B	(French)	200638	601
SPEC B	(English)	200638	42370
Total Word Count (Document A) 43856			
Total Word Count (Document B) 44025			
Total Word Count (All Documents) 87881			

01051560

SYSTEMS AND METHODS FOR MATCHING, SELECTING, NARROWCASTING, AND/OR CLASSIFYING BASED ON RIGHTS MANAGEMENT AND/OR OTHER INFORMATION
ELEKTRONISCHE VORRICHTUNG UND SYSTEM ZUR RECHTSVERWALTUNGSBASIERTEN KLASSIFIZIERUNG UND UBEREINSTIMMUNG
SYSTEMES ET PROCEDES DE COMPARAISON, DE SELECTION, DE DISTRIBUTION RESTREINTE, ET/OU DE CLASSIFICATION SELON DES DONNEES RELATIVES A UNE GESTION DES DROITS ET/OU D'AUTRES DONNEES

Patent Assignee:

- **Intertrust Technologies Corp**; (7745470)
  955 Stewart Drive; Sunnyvale CA 94085-3913; (US)
  (Proprietor designated states: all)

Inventor:

- **SHEAR, Victor, H.**
  5203 Battery Lane; Bethesda, MD 20705; (US)
- **VAN WIE, David, M.**
  Apartment 216,965 East E1 Camino Real; Sunnyvale, CA 94087; (US)
- **WEBER, Robert, P.**
  215 Waverley Street, Apt. 4; Menlo Park, CA 94025; (US)

Legal Representative:

- **Smith, Norman Ian (36041)**
  fJ CLEVELAND 40-43 Chancery Lane; London WC2A 1JQ; (GB)

	Country	Number	Kind	Date

	Country	Number	Kind	Date	
Patent	EP	1027674	A2	20000816	(Basic)
	EP	1027674	B1	20070207	
	WO	1999024928		19990520	
Application	EP	98956642		19981106	
	WO	98US23648		19981106	
Priorities	US	965185		19971106	

Designated States:
AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LI; LU; MC; NL; PT; SE;

Related Divisions: Patent (Application):EP 1501032 (EP 2004077785)

International Patent Class (V7): G06F-017/60

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06Q-0010/00	A	I	F	B	20060101	20060829	H	EP

NOTE: No A-document published by EPO

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS B	(English)	200706	1488
CLAIMS B	(German)	200706	1429
CLAIMS B	(French)	200706	1765
SPEC B	(English)	200706	25134
Total Word Count (Document A) 0			
Total Word Count (Document B) 29816			
Total Word Count (All Documents) 29816			

00936717

TRUSTED INFRASTRUCTURE SUPPORT SYSTEMS, METHODS AND TECHNIQUES FOR SECURE ELECTRONIC COMMERCE, ELECTRONIC TRANSACTIONS, COMMERCE PROCESS CONTROL AND AUTOMATION, DISTRIBUTED COMPUTING, AND RIGHTS MANAGEMENT
TREUHAND INFRASTRUKTUR UNTERSTUTZUNGSSYSTEME, VERFAHREN UND TECHNIKEN ZUM SICHEREN ELEKTRONISCHEN HANDEL, ELEKTRONISCHE TRANSAKTIONEN, STEUERUNG UND AUTOMATISIERUNG VON HANDELSVERFAHREN, VERTEILTE DATENVERARBEITUNG UND VERWALTEN VON RECHTEN
SYSTEME D'ASSISTANCE INFRASTRUCTURELLE ADMINISTRATIVE, PROCEDES ET TECHNIQUES SURS CONCERNANT LE COMMERCE ET LES TRANSACTIONS ELECTRONIQUES, COMMANDE ET AUTOMATISATION DES PROCESSUS COMMERCIAUX, CALCUL REPARTI ET GESTION DES REDEVANCES

Patent Assignee:

- **Intertrust Technologies Corp.**; (2434320)
  460 Oakmead Parkway; Sunnyvale, CA 94086-4708; (US)
  (Proprietor designated states: all)

Inventor:

- **SHEAR, Victor, H.**
  5203 Battery Lane; Bethesda, MD 20814; (US)
- **VAN WIE, David, M.**
  1780 East 25th Avenue; Eugene,OR 97403; (US)
- **WEBER, Robert**
  215 Waverly Street 4; Menlo Park, CA 94025; (US)

Legal Representative:

- **Smith, Norman Ian et al (36041)**
  fJ CLEVELAND 40-43 Chancery Lane; London WC2A 1JQ; (GB)

Country	Number	Kind	Date

	Country	Number	Kind	Date	
Patent	EP	974129	A1	20000126	(Basic)
	EP	974129	B1	20060816	
	WO	1998010381		19980312	
Application	EP	96932173		19960904	
	WO	96US14262		19960904	

Designated States:
AT; BE; CH; DE; DK; ES; FI; FR; GB; GR;
IE; IT; LI; LU; MC; NL; PT; SE;

Related Divisions: Patent (Application):EP 1577816 (EP 2005076225)

International Patent Class (V7): G07F-007/00; G07F-007/10; G06F-017/60

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G07F-0007/00	A	I	F	B	20060101	20060418	H	EP
G07F-0007/10	A	I	L	B	20060101	20060418	H	EP
G06Q-0030/00	A	I	L	B	20060101	20060418	H	EP

NOTE: No A-document published by EPO

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS B	(English)	200633	188
CLAIMS B	(German)	200633	193
CLAIMS B	(French)	200633	209
SPEC B	(English)	200633	65444
Total Word Count (Document A) 0			
Total Word Count (Document B) 66034			
Total Word Count (All Documents) 66034			

00803285

SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION
SYSTEME UND VERFAHREN FUR EIN SICHERES UBERTRAGUNGSMANAGEMENT UND ELEKTRONISCHERRECHTSSCHUTZ
SYSTEMES ET PROCEDES DE GESTION SECURISEE DE TRANSACTIONS ET DE PROTECTION ELECTRONIQUE DES DROITS

Patent Assignee:

- **Intertrust Technologies Corp**; (7745470)
  955 Stewart Drive; Sunnyvale CA 94085-3913; (US)
  (Proprietor designated states: all)

Inventor:

- **GINTER, Karl, L.**
  10404 43rd Avenue; Beltsville, MD 20705; (US)
- **SHEAR, Victor, H.**
  5203 Battery Lane; Bethesda, MD 20814; (US)
- **SPAHN, Francis, J.**
  2410 Edwards Avenue; El Cerrito, CA 94530; (US)
- **VAN WIE, David, M.**
  P.O. Box 5610; Eugene, OR 97405; (US)

Legal Representative:

- **Williams, Michael Ian et al (92852)**
  Fj Cleveland 40-43 Chancery Lane; London WC2A 1JQ; (GB)

	Country	Number	Kind	Date	
Patent	EP	861461	A2	19980902	(Basic)
	EP	861461	B1	20081029	
	WO	1996027155		19960906	
Application	EP	96922371		19960213	

	Country	Number	Kind	Date
	WO	96US2303		19960213
Priorities	US	388107		19950213

Designated States:
AT; BE; CH; DE; DK; ES; FR; GB; GR; IE;
IT; LI; LU; MC; NL; PT; SE;

Related Divisions: Patent (Application):EP 1431864 (EP 2004075701)

International Patent Class (V7): G06F-001/00; G06F-017/60;

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0021/00	A	I	F	B	20060101	20080416	H	EP
G06Q-0010/00	A	I	L	B	20060101	20080416	H	EP

NOTE: No A-document published by EPO

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS B	(English)	200844	1509
CLAIMS B	(German)	200844	1588
CLAIMS B	(French)	200844	1692
SPEC B	(English)	200844	80774
Total Word Count (Document A) 0			
Total Word Count (Document B) 85563			
Total Word Count (All Documents) 85563			

00545536

SYSTEM FOR TRACKING END-USER ELECTRONIC CONTENT USAGE
SYSTEME POUR SUIVRE L'UTILISATION DE CONTENUS ELECTRONIQUES
PAR UN UTILISATEUR FINAL

Patent Applicant/Patent Assignee:

- **INTERNATIONAL BUSINESS MACHINES CORPORATION**
- **DORAK John Jr**
- **DOWNS Edgar**
- **GRUSE George Gregory**
- **HURTADO Marco**
- **LEHMAN Christopher**
- **LOTSPIECH Jeffrey**
- **MEDINA Cesar**
- **MILSTED Kenneth**

Inventor(s):

- **DORAK John Jr**
- **DOWNS Edgar**
- **GRUSE George Gregory**
- **HURTADO Marco**
- **LEHMAN Christopher**
- **LOTSPIECH Jeffrey**
- **MEDINA Cesar**
- **MILSTED Kenneth**

	Country	Number	Kind	Date
Patent	WO	200008909	A2	20000224
Application	WO	99US18383		19990812
Priorities	US	98133519		19980813
	US	98177096		19981022

Designated States: (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR,
BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL,
IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MD, MG, MK, MN, MW,
MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG,

SI, SK, SL, TJ, TM, TR, TT, UA, UG, US,
UZ, VN, YU, ZA, ZW, AT, BE, CH, CY, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE
Language Publication Language: English

Filing Language:

Fulltext word count: 51208

00493576

SYSTEMS AND METHODS FOR MATCHING, SELECTING, NARROWCASTING, AND/OR CLASSIFYING BASED ON RIGHTS MANAGEMENT AND/OR OTHER INFORMATION
SYSTEMES ET PROCEDES DE COMPARAISON, DE SELECTION, DE DISTRIBUTION RESTREINTE, ET/OU DE CLASSIFICATION SELON DES DONNEES RELATIVES A UNE GESTION DES DROITS ET/OU D'AUTRES DONNEES

Patent Applicant/Patent Assignee:

- **INTERTRUST TECHNOLOGIES CORP**

Inventor(s):

- **SHEAR Victor H**
- **VAN WIE David M**
- **WEBER Robert P**

	Country	Number	Kind	Date
Patent	WO	9924928	A2	**19990520**
Application	WO	98US23648		19981106
Priorities	US	97965185		19971106

Designated States: (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY,
CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI,
GB, GE, GH, GM, HR, HU, ID, IL, IS, JP,
KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,
LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ,
PL, PT, RO, RU, SD, SE, SG, SI, SK, SL,
TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW,
GH, GM, KE, LS, MW, SD, SZ, UG, ZW, AM,
AZ, BY, KG, KZ, MD, RU, TJ, TM, AT, BE,
CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE, BF, BJ, CF, CG,
CI, CM, GA, GN, GW, ML, MR, NE, SN, TD,
TG

Language Publication Language: English

Filing Language:

Fulltext word count: 46172

00419920

TRUSTED INFRASTRUCTURE SUPPORT SYSTEMS, METHODS AND TECHNIQUES FOR SECURE ELECTRONIC COMMERCE, ELECTRONIC TRANSACTIONS, COMMERCE PROCESS CONTROL AND AUTOMATION, DISTRIBUTED COMPUTING, AND RIGHTS MANAGEMENT
SYSTEME D'ASSISTANCE INFRASTRUCTURELLE ADMINISTRATIVE, PROCEDES ET TECHNIQUES SURES CONCERNANT LE COMMERCE ET LES TRANSACTIONS ELECTRONIQUES, COMMANDE ET AUTOMATISATION DES PROCESSUS COMMERCIAUX, CALCUL REPARTI ET GESTION DES REDEVANCES

Patent Applicant/Patent Assignee:

- **INTERTRUST TECHNOLOGIES CORP**
- **SHEAR Victor H**
- **VAN WIE David M**
- **WEBER Robert**

Inventor(s):

- **SHEAR Victor H**
- **VAN WIE David M**
- **WEBER Robert**

	Country	Number	Kind	Date
Patent	WO	9810381	A1	19980312
Application	WO	96US14262		19960904
Priorities	WO	96US14262		19960904

Designated States: (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA,
CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE,
HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK,
LR, LS, LT, LU, LV, MD, MG, MK, MN, MW,
MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG,
SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ,
VN, KE, LS, MW, SD, SZ, UG, AM, AZ, BY,
KG, KZ, MD, RU, TJ, TM, AT, BE, CH, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE, BF, BJ, CF, CG, CI, CM, GA,
GN, ML, MR, NE, SN, TD, TG

Language Publication Language: English

Filing Language:

Fulltext word count: 85684

00418748

SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION

SYSTEMES ET PROCEDES DE GESTION DE TRANSACTIONS SECURISEES ET
DE PROTECTION DE DROITS ELECTRONIQUES

Patent Applicant/Patent Assignee:

- **INTERTRUST TECHNOLOGIES CORP**

Inventor(s):

- **GINTER Karl L**
- **SHEAR Victor H**
- **SIBERT W Olin**
- **SPAHN Francis J**
- **VAN WIE David M**

	Country	Number	Kind	Date
Patent	WO	9809209	A1	19980305
Application	WO	97US15243		19970829
Priorities	US	96706206		19960830

Designated States: (Protection type is "Patent" unless otherwise stated - for applications
prior to 2004)
AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY,
CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI,
GB, GE, GH, HU, IL, IS, JP, KE, KG, KP,
KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD,
MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO,
RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR,
TT, UA, UG, UZ, VN, YU, ZW, GH, KE, LS,
MW, SD, SZ, UG, ZW, AM, AZ, BY, KG, KZ,
MD, RU, TJ, TM, AT, BE, CH, DE, DK, ES,
FI, FR, GB, GR, IE, IT, LU, MC, NL, PT,
SE, BF, BJ, CF, CG, CI, CM, GA, GN, ML,
MR, NE, SN, TD, TG

Language Publication Language: English

Filing Language:

Fulltext word count: 195626

00344642

SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION
SYSTEMES ET PROCEDES DE GESTION SECURISEE DE TRANSACTIONS ET DE PROTECTION ELECTRONIQUE DES DROITS

Patent Applicant/Patent Assignee:

- **ELECTRONIC PUBLISHING RESOURCES INC**

Inventor(s):

- **GINTER Karl L**
- **SHEAR Victor H**
- **SPAHN Francis J**
- **VAN WIE David M**

	Country	Number	Kind	Date
Patent	WO	9627155	A2	19960906
Application	WO	96US2303		19960213
Priorities	US	95388107		19950213

Designated States: (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA,
CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE,
HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR,
LS, LT, LU, LV, MD, MG, MK, MN, MW, MX,
NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI,
SK, TJ, TM, TR, TT, UA, UG, UZ, VN, KE,
LS, MW, SD, SZ, UG, AZ, BY, KG, KZ, RU,
TJ, TM, AT, BE, CH, DE, DK, ES, FR, GB,
GR, IE, IT, LU, MC, NL, PT, SE, BF, BJ,
CF, CG, CI, CM, GA, GN, ML, MR, NE, SN,
TD, TG

? ds

```
Set     Items   Description
S1   90499905   PD<20010213
S2         11   (SECONDHAND OR (SECOND(W)HAND))(W)(CONTENT)
S3      33713   PD=20010214
S4          2   (S1 OR S3) AND S2
S5          9   (USED(W)CONTENT)(5N)(REDISTRIBUTE OR REDISTRIBUTES OR
REDI-
                STRIBUTION OR REDISTRIBUTING OR REDISTRIBUTED)
S6         25   (USED(W)CONTENT)(5N)(SALE OR SALES OR SOLD OR SELLING
OR S-
                ELLABLE)
S7          1   (USED(W)CONTENT)(5N)(RESALE OR RESALES OR RESOLD OR
RESELL-
                ING OR RESELLABLE OR RESELLER OR RESALER)
S8          0   (USED(W)CONTENT)(5N)(REDELIVER OR REDELIVERS OR
REDELIVERA-
                BLE OR REDELIVERING OR REDELIVERED)
S9          2   (S1 OR S3) AND (S5 OR S6 OR S7)
S10       195   (S1 OR S3) AND ((CONTENT)(2N)(REDISTRIBUTE OR
REDISTRIBUTES
                OR REDISTRIBUTION OR REDISTRIBUTING OR REDISTRIBUTED))
AND (-
                MUSIC OR MOVIE OR MOVIES OR AUDIO OR BOOK OR BOOKS) AND
(DIGI-
                TAL OR ELECTRONIC OR ONLINE OR INTERNET OR WEB)
S11        95   (S1 OR S3) AND ((CONTENT)(2N)(RESALE OR RESALES OR
RESOLD -
                OR RESELLING OR RESELLABLE OR RESELLER OR RESALER)) AND
(MUSIC
                OR MOVIE OR MOVIES OR AUDIO OR BOOK OR BOOKS) AND
(DIGITAL OR
                ELECTRONIC OR ELECTRONICALLY OR DIGITALLY OR ONLINE OR
INTER-
                NET OR WEB)
S12        10   (S1 OR S3) AND ((CONTENT)(2N)(REDELIVER OR REDELIVERS
OR R-
                EDELIVERABLE OR REDELIVERING OR REDELIVERED OR
REDELIVERY)) A-
                ND (MUSIC OR MOVIE OR MOVIES OR AUDIO OR BOOK OR BOOKS)
AND (-
                DIGITAL OR ELECTRONIC OR ELECTRONICALLY OR DIGITALLY OR
ONLINE
                OR INTERNET OR WEB)
S13       300   S10 OR S11 OR S12
S14        32   S13 AND (RIGHT OR RIGHTS) AND (USEAGE OR USAGES OR TERM
OR
```

```
                TERMS) AND (LICENSE OR LICENSES OR LICENSING OR LICENSED)
S15        26   RD  (unique items)
```

? s s15 and (secondhand or second(w)hand or used)

Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
```
Processed  10 of  51 files ...
Processing
Processed  30 of  51 files ...
Processing
Processing
Processed  50 of  51 files ...
Processing
Completed processing all files
             26   S15
          61432   SECONDHAND
       26971319   SECOND
        9263227   HAND
         136052   SECOND(W)HAND
       28248675   USED
S16        21   S15 AND (SECONDHAND OR SECOND(W)HAND OR USED)
```

? s s15 and ((secondhand or second(w)hand or reuse or reuses or reused or reusing or used)(2n)(content or movie or movies or audio or music or book or books or ebook or ebooks))

Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing

Processing
Processing
Processing
Processing
Processing
Processing
Processed 10 of 51 files ...
Processing
Processing
Processed 20 of 51 files ...
Processing
Processed 30 of 51 files ...
Processing
Processed 40 of 51 files ...
Processing
Processing
Processed 50 of 51 files ...
Processing
Completed processing all files
              26 S15
           61432 SECONDHAND
        26971319 SECOND
         9263227 HAND
          136052 SECOND(W)HAND
          282527 REUSE
            8369 REUSES
          130967 REUSED
           47582 REUSING
        28248675 USED
         7505470 CONTENT
         2572337 MOVIE
         1523805 MOVIES
         2925444 AUDIO
         5639748 MUSIC
         7941162 BOOK
         5111975 BOOKS
           18444 EBOOK
           13641 EBOOKS
          177870 (((((SECONDHAND OR SECOND(W)HAND) OR REUSE) OR
REUSES)
                  OR REUSED) OR REUSING) OR USED)(2N)(((((((CONTENT OR
                  MOVIE) OR MOVIES) OR AUDIO) OR MUSIC) OR BOOK) OR
BOOKS)
                  OR EBOOK) OR EBOOKS)
     S17   17 S15 AND ((SECONDHAND OR SECOND(W)HAND OR REUSE OR
REUSES
                  OR REUSED OR REUSING OR USED)(2N)(CONTENT OR MOVIE OR
                  MOVIES OR AUDIO OR MUSIC OR BOOK OR BOOKS OR EBOOK OR
                  EBOOKS))

? rd

>>>Duplicate detection is not supported for File 347.

>>>Duplicate detection is not supported for File 348.

```
>>>Duplicate detection is not supported for File 349.

>>>Records from unsupported files will be retained in the RD set.
     S18     17  RD  (unique items)
```

? t s18/3/all

18/3/1 (Item 1 from file: 20)
DIALOG(R)File 20: Dialog Global Reporter
(c) 2009 Dialog. All rights reserved.

05061354 **(USE FORMAT 7 OR 9 FOR FULLTEXT)**
Digital Watermarking: The Copyright Crawlers

COMPUTERS TODAY , p 90
April 30, 1999
Journal Code: WCOT   **Language:** English   **Record Type:** FULLTEXT
Word Count: 1540

18/3/2 (Item 1 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)
(c) 2009 ProQuest Info&Learning. All rights reserved.

02358067   115921677
Being negligent and liable: a challenge for information professionals

Hannabuss, Stuart
Library Management   v21n6 pp: 316-329
2000
ISSN: 0143-5124 **Journal Code:** LBM
Word Count: 9693

18/3/3 (Item 1 from file: 16)
DIALOG(R)File 16: Gale Group PROMT(R)
(c) 2009 Gale/Cengage. All rights reserved.

07052886   **Supplier Number:** 58378495 **(USE FORMAT 7 FOR FULLTEXT)**

**Using the Web to relieve permissions bottlenecks : Yankee, iCopyright take
different tacks to same end.(Yankee Book Peddler)(Company Business and
Marketing)**
Votsch, Victor; Walter, Mark
The Seybold Report on Internet Publishing , v 3 , n 11 , p NA
July , 1999
Language: English   **Record Type:** Fulltext
Document Type: Newsletter ; Trade

Word Count: 1692

18/3/4 (Item 1 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

12361278   **Supplier Number:** 62599337 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Making Smart Licensing Decisions.

guenther, kim
Computers in Libraries , 20 , 6 , 58
June , 2000
ISSN: 1041-7915
Language: English
Record Type: Fulltext
Word Count: 2445   **Line Count:** 00207

18/3/5 (Item 1 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

02416312   **Supplier Number:** 62599337 (**Use Format 7 Or 9 For** FULL TEXT)
Making Smart Licensing Decisions.(Industry Trend or Event)

guenther, kim
Computers in Libraries , 20 , 6 , 58
June , 2000
ISSN: 1041-7915
Language: English   **Record Type:** Fulltext
Word Count: 2445   **Line Count:** 00207

Dialog eLink: Order File History
18/3/6 (Item 1 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

01289339

Digital content distribution using web broadcasting services
Verbreitung digitalen Inhalts unter Benutzung eines Internet-Sendeservices
Distribution de contenu numerique utilisant un service de diffusion de donnees

Patent Assignee:

- **International Business Machines Corporation**; (200128)
  New Orchard Road; Armonk, NY 10504; (US)
  (Applicant designated States: all)

Inventor:

- **Mourad, Magda, c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)
- **Munson, Jonathan P., c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)
- **Pacifici, Giovanni, c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)
- **Tantawy, Ahmed, c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)
- **Youssef, Alaa S., c/o IBM United Kingdom Ltd.**
  Intellectual Property Law, Hursley Park; Winchester, Hampshire SO21 2JN; (GB)

Legal Representative:

- **Ling, Christopher John (80401)**
  IBM United Kingdom Limited, Intellectual Property Department, Hursley Park;
  Winchester, Hampshire SO21 2JN; (GB)

	Country	Number	Kind	Date	
Patent	EP	1107137	A2	20010613	(Basic)
	EP	1107137	A3	20040428	
Application	EP	2000310981		20001208	
Priorities	US	457563		19991209	
	US	487417		20000120	

Designated States:
AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LI; LU; MC; NL; PT; SE; TR;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-017/30**Abstract Word Count:** 151
NOTE: 18
NOTE: Figure number on first page: 18

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English

Procedural: English

Application: English

Fulltext Availability	Available Text	Language	Update	Word Count
CLAIMS A		(English)	200124	1260
SPEC A		(English)	200124	46736
Total Word Count (Document A) 47996				
Total Word Count (Document B) 0				
Total Word Count (All Documents) 47996				

01276898

CONTENTS MANAGEMENT SYSTEM, DEVICE, METHOD, AND PROGRAM STORAGE MEDIUM
INHALTSVERWALTUNGSSYSTEM, VORRICHTUNG, VERFAHREN UND PROGRAMMSPEICHERMEDIUM
SYSTEME, DISPOSITIF, PROCEDE ET SUPPORT DE PROGRAMME POUR LA GESTION DE CONTENUS

Patent Assignee:

- **Sony Corporation**; (214028)
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
  (Applicant designated States: all)

Inventor:

- **ISHIBASHI, Yoshihito, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)

- **OHISHI, Tateo, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **MUTO, Akihiro, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **KITAHARA, Jun, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **SHIRAI, Taizou, Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)

Legal Representative:

- **DeVile, Jonathan Mark, Dr. et al (91151)**
  D. Young & Co 21 New Fetter Lane; London EC4A 1DA; (GB)

	Country	Number	Kind	Date	
Patent	EP	1128598	A1	20010829	(Basic)
	WO	200119017		20010315	
Application	EP	2000956997		20000907	
	WO	2000JP6089		20000907	
Priorities	JP	99253660		19990907	
	JP	99253661		19990907	
	JP	99253662		19990907	
	JP	99253663		19990907	
	JP	99260638		19990914	
	JP	99264082		19990917	
	JP	99265866		19990920	

Designated States:
DE; FR; GB;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): H04L-009/32; G06F-015/00; H04N-005/91; G11B-020/10; G10K-015/04; H04N-007/167**Abstract Word Count:** 172
NOTE: 0020
NOTE: Figure number on first page: 0020

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: Japanese

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200135	29406
SPEC A	(English)	200135	83907
Total Word Count (Document A) 113313			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 113313			

Dialog eLink: Order File History
18/3/8 (Item 3 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2009 European Patent Office. All rights reserved.

01273919

**INFORMATION TRANSMISSION SYSTEM, TRANSMITTER, AND
TRANSMISSION METHOD AS WELL AS INFORMATION RECEPTION
SYSTEM, RECEIVER AND RECEPTION METHOD**
INFORMATIONSUBERTRAGUNGSSYSTEM, SENDER,
UBERTRAGUNGSVERFAHREN, SOWIE INFORM ATIONSEMPFANGSSYSTEM,
EMPFANGER UND EMPFANGSVERFAHREN
SYSTEME DE TRANSMISSION D'INFORMATIONS, EMETTEUR ET
RECEPTEUR, PROCEDE DE TRANSMISSION D'INFORMATIONS, PROCEDE DE
RECEPTION D'INFORMATIONS

Patent Assignee:

* **Sony Corporation**; (214028)
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
  (Applicant designated States: all)

Inventor:

* **ISHIBASHI, Yoshihito, c/o Sony Corporation**
  6-7-35, Kitashinagawa, Shinagawa-ku; Tokyo 141-0001; (JP)
* **OHISHI, Tateo, c/o Sony Corporation**
  6-7-35, Kitashinagawa-ku; Shinagawa-ku, Tokyo 141-0001; (JP)

- **MATSUYAMA, Shinako, c/o Sony Corporation**
  6-7-35, Kitashigawa, Shinagawa-ku; Tokyo 141-0001; (JP)
- **ASANO, Tomoyuki, c/o Sony Corporation**
  7-35, Kitashigawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **MUTO, Akihiro, c/o Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)
- **KITAHARA, Jun, c/o Sony Corporation**
  7-35, Kitashinagawa 6-chome, Shinagawa-ku; Tokyo 141-0001; (JP)

Legal Representative:

- **Pilch, Adam John Michael et al (50481)**
  D. YOUNG & CO., 21 New Fetter Lane; London EC4A 1DA; (GB)

	Country	Number	Kind	Date	
Patent	EP	1134670	A1	20010919	(Basic)
	WO	200116776		20010308	
Application	EP	2000955022		20000825	
	WO	2000JP5742		20000825	
Priorities	JP	99242294		19990827	
	JP	99242295		19990827	
	JP	99242296		19990827	
	JP	99283326		19990827	

Designated States:
DE; FR; GB;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-015/00; G06F-017/60; H04L-009/08; G10K-015/02**Abstract Word Count:** 214
NOTE: 20
NOTE: Figure number on first page: 20

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: Japanese

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200138	14242
SPEC A	(English)	200138	53309
Total Word Count (Document A) 67551			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 67551			

01257209

Method and apparatus for uniquely identifying a customer purchase in an electronic distribution system
Verfahren und Apparat zum eindeutigen Identifizieren eines Kundeneinkaufs in einem elektronischen Auslieferungs-System
Methode et appareil pour l'identification unique d'un achat d'un client dans un systeme de distribution electronique

Patent Assignee:

- **Wistron Corporation**; (7754890)
  21 F, No. 88, Sec. 1 Hsin-Tai-Wu Road Hsi-Chih City; Taipei Hsien 221; (TW)
  (Proprietor designated states: all)

Inventor:

- **Dorak, John J., Jr.,c/o IBM United Kingdom Ltd**
  Intel. Property Law,Hursley Park; Winchester,Hampshire S021 2JN; (GB)

Legal Representative:

- **Schaeberle, Steffen et al (93211)**
  Hoefer & Partner Patentanwalte Pilgersheimer Strasse 20; 81543 Munchen; (DE)

	Country	Number	Kind	Date	
Patent	EP	1085443	A2	20010321	(Basic)
	EP	1085443	A3	20050105	
	EP	1085443	B1	20080827	
Application	EP	2000308024		20000914	
Priorities	US	397419		19990917	

Designated States:
AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LI; LU; MC; NL; PT; SE;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-017/60

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0021/00	A	I	F	B	20060101	20080226	H	EP

Abstract Word Count: 123
NOTE: 18
NOTE: Figure number on first page: 18

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English

Procedural: English

Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200112	694
SPEC A	(English)	200112	42226
CLAIMS B	(English)	200835	1047
CLAIMS B	(German)	200835	1107
CLAIMS B	(French)	200835	1243
SPEC B	(English)	200835	43289
Total Word Count (Document A) 42927			
Total Word Count (Document B) 46686			
Total Word Count (All Documents) 89613			

01245941

Secure electronic content distribution on CDS and DVDS
Sichere Verteilung von elektronischem Inhalt auf CDs und DVDs
Distribution securisee d'un contenu electronique sur CDs et DVDs

Patent Assignee:

- **International Business Machines Corporation**; (200129)
  New Orchard Road; Armonk, NY 10504; (US)
  (Proprietor designated states: all)

Inventor:

- **Hurtado, Marco M.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Milsted, Kenneth L.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Gruse, George G.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Downs, Edgar,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Lehman, Christopher T.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Spagna, Richard L.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)
- **Lotspiech, Jeffrey B.,c/o IBM United Kingdom Ltd**
  Intellectual Property Law,Hursley Park; Winchester,Hampshire SO21 2JN; (GB)

Legal Representative:

- **Ling, Christopher John (80401)**
  IBM United Kingdom Limited, Intellectual Property Department, Hursley Park;
  Winchester,Hampshire SO21 2JN; (GB)

	Country	Number	Kind	Date	
Patent	EP	1077398	A1	20010221	(Basic)
	EP	1077398	B1	20060920	
Application	EP	2000305655		20000705	
Priorities	US	376102		19990817	

Designated States:
AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LI; LU; MC; NL; PT; SE;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-001/00; H04L-029/06

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0001/00	A	I	F	B	20060101	20001128	H	EP
H04L-0029/06	A	I	L	B	20060101	20001128	H	EP

Abstract Word Count: 211
NOTE: 18
NOTE: Figure number on first page: 18

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English

Procedural:	English
Application:	English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200108	981
SPEC A	(English)	200108	42868
CLAIMS B	(English)	200638	520
CLAIMS B	(German)	200638	534
CLAIMS B	(French)	200638	601
SPEC B	(English)	200638	42370
Total Word Count (Document A) 43856			
Total Word Count (Document B) 44025			
Total Word Count (All Documents) 87881			

01051560

SYSTEMS AND METHODS FOR MATCHING, SELECTING, NARROWCASTING, AND/OR CLASSIFYING BASED ON RIGHTS MANAGEMENT AND/OR OTHER INFORMATION
ELEKTRONISCHE VORRICHTUNG UND SYSTEM ZUR RECHTSVERWALTUNGSBASIERTEN KLASSIFIZIERUNG UND UBEREINSTIMMUNG
SYSTEMES ET PROCEDES DE COMPARAISON, DE SELECTION, DE DISTRIBUTION RESTREINTE, ET/OU DE CLASSIFICATION SELON DES DONNEES RELATIVES A UNE GESTION DES DROITS ET/OU D'AUTRES DONNEES

Patent Assignee:

- **Intertrust Technologies Corp**; (7745470)
  955 Stewart Drive; Sunnyvale CA 94085-3913; (US)
  (Proprietor designated states: all)

Inventor:

- **SHEAR, Victor, H.**
  5203 Battery Lane; Bethesda, MD 20705; (US)
- **VAN WIE, David, M.**
  Apartment 216,965 East E1 Camino Real; Sunnyvale, CA 94087; (US)
- **WEBER, Robert, P.**
  215 Waverley Street, Apt. 4; Menlo Park, CA 94025; (US)

Legal Representative:

- **Smith, Norman Ian (36041)**
  fJ CLEVELAND 40-43 Chancery Lane; London WC2A 1JQ; (GB)

	Country	Number	Kind	Date

	Country	Number	Kind	Date	
Patent	EP	1027674	A2	20000816	(Basic)
	EP	1027674	B1	20070207	
	WO	1999024928		19990520	
Application	EP	98956642		19981106	
	WO	98US23648		19981106	
Priorities	US	965185		19971106	

Designated States:
AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LI; LU; MC; NL; PT; SE;

Related Divisions: Patent (Application):EP 1501032 (EP 2004077785)

International Patent Class (V7): G06F-017/60

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06Q-0010/00	A	I	F	B	20060101	20060829	H	EP

NOTE: No A-document published by EPO

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS B	(English)	200706	1488
CLAIMS B	(German)	200706	1429
CLAIMS B	(French)	200706	1765
SPEC B	(English)	200706	25134
Total Word Count (Document A) 0			
Total Word Count (Document B) 29816			
Total Word Count (All Documents) 29816			

00803285

SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION
SYSTEME UND VERFAHREN FUR EIN SICHERES UBERTRAGUNGSMANAGEMENT UND ELEKTRONISCHERRECHTSSCHUTZ
SYSTEMES ET PROCEDES DE GESTION SECURISEE DE TRANSACTIONS ET DE PROTECTION ELECTRONIQUE DES DROITS

Patent Assignee:

- **Intertrust Technologies Corp**; (7745470)
  955 Stewart Drive; Sunnyvale CA 94085-3913; (US)
  (Proprietor designated states: all)

Inventor:

- **GINTER, Karl, L.**
  10404 43rd Avenue; Beltsville, MD 20705; (US)
- **SHEAR, Victor, H.**
  5203 Battery Lane; Bethesda, MD 20814; (US)
- **SPAHN, Francis, J.**
  2410 Edwards Avenue; El Cerrito, CA 94530; (US)
- **VAN WIE, David, M.**
  P.O. Box 5610; Eugene, OR 97405; (US)

Legal Representative:

- **Williams, Michael Ian et al (92852)**
  Fj Cleveland 40-43 Chancery Lane; London WC2A 1JQ; (GB)

	Country	Number	Kind	Date	
Patent	EP	861461	A2	19980902	(Basic)
	EP	861461	B1	20081029	
	WO	1996027155		19960906	
Application	EP	96922371		19960213	

	Country	Number	Kind	Date
	WO	96US2303		19960213
Priorities	US	388107		19950213

Designated States:
AT; BE; CH; DE; DK; ES; FR; GB; GR; IE;
IT; LI; LU; MC; NL; PT; SE;

Related Divisions: Patent (Application):EP 1431864 (EP 2004075701)

International Patent Class (V7): G06F-001/00; G06F-017/60;

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0021/00	A	I	F	B	20060101	20080416	H	EP
G06Q-0010/00	A	I	L	B	20060101	20080416	H	EP

NOTE: No A-document published by EPO

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English

Procedural:	English
Application:	English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS B	(English)	200844	1509
CLAIMS B	(German)	200844	1588
CLAIMS B	(French)	200844	1692
SPEC B	(English)	200844	80774
Total Word Count (Document A) 0			
Total Word Count (Document B) 85563			
Total Word Count (All Documents) 85563			

SYSTEM FOR TRACKING END-USER ELECTRONIC CONTENT USAGE
SYSTEME POUR SUIVRE L'UTILISATION DE CONTENUS ELECTRONIQUES
PAR UN UTILISATEUR FINAL

Patent Applicant/Patent Assignee:

- **INTERNATIONAL BUSINESS MACHINES CORPORATION**
- **DORAK John Jr**
- **DOWNS Edgar**
- **GRUSE George Gregory**
- **HURTADO Marco**
- **LEHMAN Christopher**
- **LOTSPIECH Jeffrey**
- **MEDINA Cesar**
- **MILSTED Kenneth**

Inventor(s):

- **DORAK John Jr**
- **DOWNS Edgar**
- **GRUSE George Gregory**
- **HURTADO Marco**
- **LEHMAN Christopher**
- **LOTSPIECH Jeffrey**
- **MEDINA Cesar**
- **MILSTED Kenneth**

	Country	Number	Kind	Date
Patent	WO	200008909	A2	20000224
Application	WO	99US18383		19990812
Priorities	US	98133519		19980813
	US	98177096		19981022

Designated States: (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR,
BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL,
IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MD, MG, MK, MN, MW,
MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG,

SI, SK, SL, TJ, TM, TR, TT, UA, UG, US,
UZ, VN, YU, ZA, ZW, AT, BE, CH, CY, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE
Language Publication Language: English

Filing Language:

Fulltext word count: 51208

00493576

SYSTEMS AND METHODS FOR MATCHING, SELECTING, NARROWCASTING, AND/OR CLASSIFYING BASED ON RIGHTS MANAGEMENT AND/OR OTHER INFORMATION
SYSTEMES ET PROCEDES DE COMPARAISON, DE SELECTION, DE DISTRIBUTION RESTREINTE, ET/OU DE CLASSIFICATION SELON DES DONNEES RELATIVES A UNE GESTION DES DROITS ET/OU D'AUTRES DONNEES

Patent Applicant/Patent Assignee:

- **INTERTRUST TECHNOLOGIES CORP**

Inventor(s):

- **SHEAR Victor H**
- **VAN WIE David M**
- **WEBER Robert P**

	Country	Number	Kind	Date
Patent	WO	9924928	A2	**19990520**
Application	WO	98US23648		19981106
Priorities	US	97965185		19971106

Designated States: (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY,
CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI,
GB, GE, GH, GM, HR, HU, ID, IL, IS, JP,
KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,
LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ,
PL, PT, RO, RU, SD, SE, SG, SI, SK, SL,
TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW,
GH, GM, KE, LS, MW, SD, SZ, UG, ZW, AM,
AZ, BY, KG, KZ, MD, RU, TJ, TM, AT, BE,
CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE, BF, BJ, CF, CG,
CI, CM, GA, GN, GW, ML, MR, NE, SN, TD,
TG

Language Publication Language: English

Filing Language:

Fulltext word count: 46172

00419920

TRUSTED INFRASTRUCTURE SUPPORT SYSTEMS, METHODS AND TECHNIQUES FOR SECURE ELECTRONIC COMMERCE, ELECTRONIC TRANSACTIONS, COMMERCE PROCESS CONTROL AND AUTOMATION, DISTRIBUTED COMPUTING, AND RIGHTS MANAGEMENT
SYSTEME D'ASSISTANCE INFRASTRUCTURELLE ADMINISTRATIVE, PROCEDES ET TECHNIQUES SURES CONCERNANT LE COMMERCE ET LES TRANSACTIONS ELECTRONIQUES, COMMANDE ET AUTOMATISATION DES PROCESSUS COMMERCIAUX, CALCUL REPARTI ET GESTION DES REDEVANCES

Patent Applicant/Patent Assignee:

- **INTERTRUST TECHNOLOGIES CORP**
- **SHEAR Victor H**
- **VAN WIE David M**
- **WEBER Robert**

Inventor(s):

- **SHEAR Victor H**
- **VAN WIE David M**
- **WEBER Robert**

	Country	Number	Kind	Date
Patent	WO	9810381	A1	19980312
Application	WO	96US14262		19960904
Priorities	WO	96US14262		19960904

Designated States: (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA,
CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE,
HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK,
LR, LS, LT, LU, LV, MD, MG, MK, MN, MW,
MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG,
SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ,
VN, KE, LS, MW, SD, SZ, UG, AM, AZ, BY,
KG, KZ, MD, RU, TJ, TM, AT, BE, CH, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE, BF, BJ, CF, CG, CI, CM, GA,
GN, ML, MR, NE, SN, TD, TG

Language Publication Language: English

Filing Language:

Fulltext word count: 85684

00418748

SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION

SYSTEMES ET PROCEDES DE GESTION DE TRANSACTIONS SECURISEES ET
DE PROTECTION DE DROITS ELECTRONIQUES

Patent Applicant/Patent Assignee:

- **INTERTRUST TECHNOLOGIES CORP**

Inventor(s):

- **GINTER Karl L**
- **SHEAR Victor H**
- **SIBERT W Olin**
- **SPAHN Francis J**
- **VAN WIE David M**

	Country	Number	Kind	Date
Patent	WO	9809209	A1	19980305
Application	WO	97US15243		19970829
Priorities	US	96706206		19960830

Designated States: (Protection type is "Patent" unless otherwise stated - for applications
prior to 2004)
AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY,
CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI,
GB, GE, GH, HU, IL, IS, JP, KE, KG, KP,
KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD,
MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO,
RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR,
TT, UA, UG, UZ, VN, YU, ZW, GH, KE, LS,
MW, SD, SZ, UG, ZW, AM, AZ, BY, KG, KZ,
MD, RU, TJ, TM, AT, BE, CH, DE, DK, ES,
FI, FR, GB, GR, IE, IT, LU, MC, NL, PT,
SE, BF, BJ, CF, CG, CI, CM, GA, GN, ML,
MR, NE, SN, TD, TG

Language Publication Language: English

Filing Language:

Fulltext word count: 195626

00344642

SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION
SYSTEMES ET PROCEDES DE GESTION SECURISEE DE TRANSACTIONS ET DE PROTECTION ELECTRONIQUE DES DROITS

Patent Applicant/Patent Assignee:

* **ELECTRONIC PUBLISHING RESOURCES INC**

Inventor(s):

* **GINTER Karl L**
* **SHEAR Victor H**
* **SPAHN Francis J**
* **VAN WIE David M**

	Country	Number	Kind	Date
Patent	WO	9627155	A2	19960906
Application	WO	96US2303		19960213
Priorities	US	95388107		19950213

Designated States: (Protection type is "Patent" unless otherwise stated - for applications prior to 2004)
AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA,
CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE,
HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR,
LS, LT, LU, LV, MD, MG, MK, MN, MW, MX,
NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI,
SK, TJ, TM, TR, TT, UA, UG, UZ, VN, KE,
LS, MW, SD, SZ, UG, AZ, BY, KG, KZ, RU,
TJ, TM, AT, BE, CH, DE, DK, ES, FR, GB,
GR, IE, IT, LU, MC, NL, PT, SE, BF, BJ,
CF, CG, CI, CM, GA, GN, ML, MR, NE, SN,
TD, TG

? t s18/k/all

(USE FORMAT 7 OR 9 FOR FULLTEXT)
Digital Watermarking: The Copyright Crawlers

-

It is often said that, on the **Internet,** information "wants" to be
free. Regardless of what information wants, however, those who own it
often
disagree. Writers, photographers, musicians, and artists are among
those
who have taken advantage of the worldwide publishing opportunities
provided
by the **Internet,** yet these same people are frequently being taken
advantage of by **online** pirates. Given the ease with which
audio and visual files can be duplicated, it is no surprise that
such duplication on the Net regularly occurs without the owners'
permission.
      Recently, Microsoft filed a suit against operators of **Web** sites
offering pirated office products, and the **music** industry has begun
to worry about **Internet music** archives cutting into sales.
Vendors of clip art watch in dismay as unauthorised **Web** sites reuse
their wares. Is there a way to protect intellectual property?
A number of technologies stand sentinel over **digital** content,
allowing content creators to protect their intellectual property
rights in the free-for-all of the **Internet.** In some cases,
the content can still be free for all, but the creator can track where
it's
being used. In other cases, developers can include business rules and
payment provisos with their content.
      One such new weapon to enforce the law in the **online** world is
digital watermarking. Sometimes called "fingerprinting",
digital watermarking allows copyright owners to incorporate into
their work identifying information invisible to the human eye. When
combined with new tracking services offered by some of the same
companies
that provide the watermarking technology, copyright owners can, in
theory,
find all illegal copies of their photos and **music** on the
Internet and take appropriate legal action.

For Webmasters, **digital** watermarking can help ensure that only lawful image and **audio** files are **used**, protecting Webmasters against the dangers of copyright infringement. To understand why **digital** watermarking should be seen as a benefit and not a menace to Webmasters, it is first important to understand what this new technology
provides.
A...

...dates back to the Middle Ages, when Italian papermakers marked their unique pieces of paper to prevent others from falsely claiming craftsmanship. In fact, the **term "digital** watermark" is derived from the traditional watermarks that exist in high-quality letterhead and certain currency. On letterhead, watermarks typically are
not apparent to the...

...a silent sign of quality. On certain currency, watermarks are imbedded
into paper bills, ensuring the currency holder that the bill is not counterfeit.
Similarly, **digital** watermarks also serve the purposes of identifying quality and assuring authenticity. A graphic or **audio** file bearing a **digital** watermark can inform the viewer or listener who owns the **rights** to the item. Digimarc, the self-described "leader in **digital** watermark technology," describes the process this way: "It is invisible to the naked eye. It hides in the naturally occurring
variations throughout images. Imbed a **digital** watermark in images and create a copyright communication device. Anyone who views your watermarked image with your unique identifier will know your identity."
Since early...

...trademark on the original image. The average trademark has more than 1,00,000 pixels, as per to Michel Bezy, program manager for IBM's **Digital** Library products.
Bezy notes that watermarks can have useful purposes other than copyright protection. For instance, one could include metadata about a photograph-the photographer...

...camera type, the date and time of the exposure-along with the image itself. The data about the photograph would be encoded internally with the
digital rendition.
The magazine Playboy has a very real problem with picture pirates. Playboy Enterprises is responsible for some most popular sites, including a
new Cyber...

...photography, and repurpose them as a front door to pornography sites."
Playboy uses Digimarc's invisible watermarking scheme and MarcSpider service to ferret out offenders.
Digital Branding Irons
Audio files also can fall prey to Net pirates. Using RealAudio, content providers can add copyright information and create listen-only

files that aren't downloaded to a user's hard drive. But to let users save
CD-quality **audio** files yet prevent them from **redistributing**
the files, **content** providers can turn to companies like Liquid
Audio, which develops software to make **online music**
distribution both easier and safer.

Also pursuing **online music** piracy is Broadcast
Music Inc. (BMI), the performing **rights** organisation that
represents more than 2,00,000 copyright holders including songwriters,
composers and **music** publishers. BMI recently introduced MusicBot-"a
new **Web** robot designed to gather market information and **music**
trends while monitoring the use of **music** in cyberspace." A similar
service, Digimarc's MarcSpider, combs the **Web** for images imbedded
with **digital** watermarks, providing copyright owners with information
on where their images appear (with or without permission) on the
Internet.

Riding into the Net Frontier

While **digital** watermarks and tracking technologies are
receiving great praise, these tools still are in their infancy.
Digital watermarks are subject to stripping, and tracking is limited
to non-password protected sites.

Despite claims that **digital** watermarks can survive image
alteration and cannot be stripped without seriously affecting image
quality, a recent CyberTimes report revealed that the **digital**
watermarks on some images "may have been weakened or (may have)
disappeared
by the time the images were processed for the **Internet**." Resizing,
compressing and converting images from one file type to another may add
noise to an image or diminish its watermark in such a manner that the
mark
becomes unreadable.

However, if watermarking content develops into a universally
addressable format, then we very well may reach a threshold at which
digital "copyright cops" could begin to ride the **Web** checking
up on everyone's **rights** to publish.

BOX 1

Watermarking Tools

The clearance tools in the hands of honest **Web** publishers

Argent. The patented technology can be simply differentiated from
other **digital** watermark systems by its use of "keys" in the
watermark process.

Cognicity. Provides data embedding (or **digital** watermarking)
solutions across **audio**, video and image-all rich media data types-
for such applications as broadcast monitoring, IP protection and
Internet promotion.

Copysight. A multi-platform service designed to allow customers to
assert and safeguard their intellectual property (graphics, text, Java
applets, cgi programs, **audio** files, etc.) against **Internet**
pirates.

EIKONAmark. Transforms the copyright owner id number into an
invisible
watermark and casts it in the body of the image. The watermark can be
detected by the copyright owner by using EIKONAmark. For Windows
3.x/Windows 95.

Giovanni. Offers both image and **audio** watermarking technology
combining a secure key architecture with an embedded signalling
algorithm.

```
    JK...

...is available in form of compressed binaries for Windows 95, SGI, Sun
and
Linux.
      Musicode. Musicode embeds inaudible, indelible, and easily-
recoverable
copyright information within music. These copyright watermarks can
survive multiple analogue tape generations as well as radio broadcast
without altering the fidelity of the recording. By ARIS Technologies.
      Digmarc. A plug-in for graphics packages such as Adobe Photoshop,
Adobe PhotoPaint and CorelDRAW. Allows the creation and tracking of
watermarked digital images. By Digimarc.
      PixelTag. Allows many bits of copyright, caption, or tagging
information to be imperceptibly embedded in images and other media. The
hidden information resides in the actual pixel brightness values, not
in
details of the digital representation, so the hidden information
stays with the image despite changes in file format (TIFF to JPEG), or
digital-to-analogue conversion (printing).
      StirMark. A generic tool for simple robustness testing of image
watermarking algorithms and other steganographic techniques
(anti-watermarking software).
      SureSign. SureSign fingerprints can be embedded into graphic,
audio, and video digital data files to carry information
relating to ownership and revision status. Used in the field of
copyright/IPR protection and also to validate and authenticate material
in
applications such as security documents and electronic commerce.
      SysCoP. Online watermarking service that allows the information
provider to embed a robust copyright label in image or video data.
Rather
than attempt to prevent the illicit...
...for Windows 95 and Linux.
      BOX 2
      Digimarc-ing IT
      1. Artist encodes image with a Digimarc ID.
      2. Watermarked image is posted on the Web.
      3. ID information is visible when the watermarked image is
downloaded
and opened with a Digimarc reader; Digimarc's Web site includes a
directory that links the ID with the artist's contact info.
      4. Digimarc's MarcSpider crawls the Web looking for watermarked
images and reporting unauthorised uses.
```

Descriptors: ...Patents **Licensing** & Standards...
Country Names/Codes:
19990430

18/K/2 (Item 1 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)

Abstract:

...information professionals to issues of professional negligence and liability. In this paper, key legal issues are discussed, and negligence
and liability is examined in the **electronic** domain. It is suggested that the commercialisation of the information marketplace and growing awareness of negligence and liability issues are encouraging information
professionals to look...

Text:

...some of these issues as they apply to information and library professionals, arguing that the increasing commodification of information
products and services, the growth of **electronic** information availability, and increased professional awareness about liability and insurance, has placed information liability centre stage in professional
practice. The scale of discussion, above all on the **Internet**, gives historiographic proof of this interest, and the growth of disclaimers on
information products and services is a further token of this trend. The hybridisation...g. between a doctor and a patient for a form of treatment),
precise details may not have been determined (unlike a contract which usually specifies **terms** and conditions).

Contractual liability

Issues of liability draw on two different areas of the law, tort (where we
have explored negligence) and contract law. Contracts...defining information liability difficult.

That said, it is clear to see that there are situations where information
is produced in copyrightably tangible forms where exclusive **rights** of exploitation can be protected, and situations where information is charged for and paid for, and provided as an exclusive product and service
under contractually...

...accepted wisdom that the provision of such products and services is not,
in the first instance, contractual in nature. Reference interviews, user
education, bibliographical advice, **online** searches may all be free. After all, for the public sector, traditionally, funding has been indirect,
implicit, and market forces have not applied in the...

...accountability, cost-effectiveness, cost centre and delegated budgeting,
and income generation has encouraged and driven services increasingly towards contractual or quasi-contractual exchanges with customers.

Online searches have high unit costs and therefore need precise
pricing. Staff time is scarce and opportunity costs have to be observed
when doing one thing...

...situation. In contract law there is, again, a duty of care, focused
on
what is to be provided and how. In contracts there are express **terms**
(e.g. X pays Y Pounds 200 for the item, delivery will take place
quarterly,
etc.) and implied **terms** (e.g. the professional will exercise
reasonable care). Reasonable care is an implicit threshold, although
there
may be more closely specified standards and specifications in...

...disclaimers we find assertions that the client, user, visitor to a
Website, should regard the information there "as is" and not assume
everything is completely **right** and then, later, when things go
wrong, come back to the supplier and blame them for incompetence.
Exclusion
clauses can be taken too far and...

...To what extent, in such circumstances, does contributory negligence
apply (e.g. where a student alleges that the very availability of
downloadable material from the **Internet** is an exoneration for their
having passed off the work of others as their own for an assignment)?

As always, information presents unique difficulties here. For example,
a
book is a product but the ideas represented in a **book** may be
defective or may mislead or may be incomplete: where does the liability
lie? For example, a library or a bookshop has a **book** or journal on
the shelf but is it, by stocking and making available for sale,
necessarily
and knowingly endorsing what the **book** or journal contains? For
example, a company passes content to an information service provider
(ISP)
for display and dissemination of the **Internet**, and material appears
framed ...transit or crashes? What if the information is provided by
one
party and the software by another? What if a Website is provided on the
Internet and links are created to it by another and then a third
party objects, say, to allegedly defamatory material there? What if
controversial content appears...
...material before transmission?

Questions like these are of particular interest and relevance to people
in
the information profession, and particularly now with the growth of
electronic information products and services. Errors, omissions,
faults in security, lost data, unfiltered content, and much else, opens
up
information liability and professional negligence to a...

...to believe that Greenmoss Builders were in administration, leading
ironically to their bankruptcy. This case highlighted in the mid-1980s
the
fine balance between the **rights** of involved parties and the

generalised benefit of having widely available financial information.
Various writers have emphasised the vulnerability of the information
chain
to events like this. **Electronic** liability is big business,
stretching from computer misuse to data protection, data encryption to
secure virtual private networks, acceptable use policies to information
indemnification.

Electronic liability

Information products and services have become much more **electronic**
or **digital.** This entails greater professional awareness about
relevant legal and ethical dimensions and implications in information
work.
Information professionals continue to play an important role as...
...and causation, duty of care and defences. In the second, there is a
noticeable increase in the use and awareness of contractual law, in the
terms and conditions, warranties and exemptions, expressed and
implied in and by contracts for the use of software and hardware.
Particular fields, like **electronic** journal publishing and
dissemination, are changing rapidly and highlight the way in which
stakeholders are vying for economic advantage and presenting new
challenges
to information providers and intermediaries (for example, in
licensing, monitoring, and remuneration).

The Library Association's information statement on information quality
and
liability flagged this back in 1994, when it said: "Information workers
should be aware of the possibility that they could be held responsible
in
the event of inaccurate or incomplete information being provided from
an
online or CD-ROM database. At worst, this could even lead to action
for damages. It is instructive to note that most suppliers of CD-ROMs
and
online hosts have taken the precaution of including liability
exclusion clauses in their contracts, thus making it appear difficult
to
take action against them." We have already considered the difficulties
of
determining responsibility in the information chain, and the
electronic information chain is more complex and unattributable
still. Speed is often regarded as more important than accuracy: at
least,
there is a trade-off. As...
...1994, where a local authority used software to administer local
finance
collection and found errors in the software).

There is increasing attention to liability and **online** and
electronic products and services. Intellectual property law
worldwide is driving some of this along. The **Digital** Millennium
Copyright Act 1998 in the USA, for instance, includes a provision which
seeks to limit the potential financial damages that **online** service
providers, including libraries and educational institutions, could face
when they function like a common carrier, allowing **online** users

access to copyrighted material placed there by someone else. Rather than
confront huge financial claims if the third party infringes someone's
copyrights, OSPs...

...American Library Association Website, dated 18 November 1998).

Elsewhere, in Canada, over the last year or so, a comprehensive study of
civil liability and the **Internet** has been carried out by Industry
Canada/Strategis. It re-emphasises the fact that liability (say for
statements made about others) is the same on the **Internet** as in
traditional documents/media. It picks out defamation, privacy and violation
of secrecy, misuse of personal information, communication of erroneous
information, and unfair competition as areas of concern. Responsibility for
resulting damages rests with the person performing the illegal act.
Problems arise on the **Internet** because other parties may intervene
(e.g. publishers, broadcasters, re-transmitters, common carriers).

One of these is the librarian: like booksellers, they distribute
information. They...Failing to do so, they can be held liable (from summary
at Strategis Website, dated 17 March 1997). This reasoning is extended to
operators of **online** services, Websites, bulletin board services, on
the **Internet**: they can be in the same situation and should moderate
the service. "It has no control over the information circulating on the
system and thus...

...censorship law and well before that.

ISPs can be found liable in a number of areas. Copyright is one of these:
e.g. violation of **right** to reproduce which belongs to the
rights-holder, placing an **electronic** copy of a best-selling
novel on their Website, allowing newsgroup servers to copy newsgroup files.
Even if they do not take part directly in...

...or contributory infringement. Doing this involves them in vicarious
liability, where someone may be liable for infringing works of another if
that someone has the **right** and ability to control the infringer's
acts and receives financial reward (if only by keeping the infringer on the
system!) from such infringement.
The...

...Netcom was not liable and merely storing and disseminating copies of
files to which the Church of Scientology objected.

Liability for copying both text and **music** (another big area) are
both changing as we speak, and open up issues of:

- negligence and contract law where information systems and provision;

- intellectual property; and

- the **right** to publish and disseminate information and knowledge in
a fair society.

With all these in play, it is no surprise that information
professionals
are looking more and more to what is strictly allowable under the law.
With
this in view, we can see an increasing trend towards observing the
terms and conditions of use. The provision and use of information
has become, in fact, contractual, and is likely to get more so. Among
the
many...in some way to wrongdoing by others (say, in a university,
providing
the means for a student to download, store and disseminate pornographic
or
paedophile **electronic** image files). Contractual matters kick in
here, too, not just in **terms** of any **terms** and conditions for
the use of the network, but also in view of the employment contract for
the
employee.

Defamation or cyberlibel is relevant here...

...A company is liable for the acts of employees taken in the course of
his
or her employment, and so is liable for consequences of **electronic**
messages on the **Internet** or sent through an internal e-mail system.
It may be regarded not as the common carrier (we have seen the
liability
conditions) but as...

...are principles worth going back to in any situation of alleged or
perceived defamation.

They are expected to take reasonable care to monitor and secure
electronic dissemination, and, if this can be demonstrated, they
have the defence (under the Defamation Act 1996) of "innocent
dissemination". What reasonable care is - and we...

...1997, chapter 10).

The players here are diverse, worldwide, and often have opposing
interests.
In some jurisdictions governments are taking action to ensure
responsibility. The **Internet** Watch Foundation, for example, founded
in 1996, had the backing of the UK Government, and undertakes to inform
all
British ISPs once they locate undesirable...

...would simply be passed on to subscribers and customers). The drift
of
legal opinion lies in removing liability from ISPs.

The many players in the **electronic** domain, then, while being equally

subject to key legal and tortious factors and principles of law, reveal
increasing degrees of awareness about liability issues.
The...jurisdiction,
is in the Anglo-American world at least taking on a common character,
probably influenced by the high percentage of US content on the
Internet.

Disclaiming liability

It comes as no surprise, given the noticeable trend towards looking at
exactly what the **terms** and conditions of the contract say (for
instance, in the site licence for software use on a university network,
or
the conditions imposed on Website visitors if they want to download or
view
a company document in Java), that these **terms** and conditions have
taken on a particular importance. They stipulate how and where the
electronic content should be **used** and stipulate
penalties and charges for deviation. Often they cover how updates and
revisions should be installed and what forms of oversight or
collaboration
they...

...the exclusion clause, seeking to exempt the supplier/producer from
liability, say, for untoward defects and any consequential harm or
loss.

In the world of **electronic** information, many if not most Websites,
and much else, contain succinct (and in some cases voluminous!)
guidelines
on the use of the material. For instance...

...regulations. Because of these differences, you should not act or
rely on
any information on this Website without seeking the advice of a
competent
attorney **licensed** to practice law in your jurisdiction for your
particular situation. The author makes no representation that materials
on
this Website are appropriate or available for...

...like trademarks, downloading for personal use only, keeping to the
law,
and being "solely liable for any damage resulting from any infringement
of
copyrights, proprietary **rights**, or any other harm resulting from
such a submission". Napier University, in Edinburgh, on their Website
state: "Whilst every effort has been made to ensure the accuracy of
information supplied on this **Web** server, Napier University cannot be
held responsible for any errors or omissions, and course and facilities
listed may be cancelled, modified or replaced at short...
...fearful of oppressive custodianship by powerful interest groups rest
assured that policing abuses is almost impossible.

The IATA (International Air Transport Association) Website reserves the
right at all times to monitor and record any activity on its site,
an interest issue (along with cookie inspections) which concern some

commentators on the grounds of privacy. The Bloomberg Website contains
extensive **terms** and conditions which visitors are asked to read
"before using the site". Continuing use of the site implies your
acceptance
of the **terms** and conditions. These include observing the law on
intellectual property, using the site for legal purposes only (e.g. not
using **content** for **resale** or passing yourself off as
Bloomberg), agreeing not to decompile or reproduce or reverse engineer
works from the site, and accept the fact that use...way for incidental
and
consequential damages resulting from any use of the information on the
Website. You are encouraged to use discretion while browsing the
Internet using the Yahoo!directory: it may direct you, it says, to
sites containing information which some people may find offensive or
inappropriate. "Yahoo!makes no...

...responsible for the accuracy, copyright compliance, legality or
decency
of material contained in sites listed in the directory or in the
materials". It asserts the **right**, in appropriate circumstances and
at its sole discretion, to terminate the accounts of users that
infringe or
otherwise violate the **rights** of others using the directory.

What often emerges from disclaimers like these is how watertight they
look.
It clearly makes sense to remind the user...

...its employees against any claim, suit, action, or other proceeding
brought against them if you can be held responsible (e.g. if you
violate
the **terms**, if someone uses your computer and accesses their Website
and does so). You admit to liability pay any costs of litigation. The
XpertSite.com Website...

...all third party claims, liability, damages and/or costs (including
but
not limited to reasonable attorneys' fees) arising from your failure to
comply with the **terms** of use, any infringement or violation of any
intellectual property or other **right** of a third party, any content,
or from your violation of any applicable law". Not only this, there are
matters of damages, too. Usually these...

...appeal of such protection. Professional liability insurance protects
you
when you are a target for a lawsuit. Companies like techinsurance.com
advertise widely on the **Internet** offering insurance solutions for
the information and computer professional: a full audit of the fast-
moving
and relevant area would be of great interest, particularly...say] but
this
must be weighed against potential claims for damages".
With the various – and ever changing – factors involved in the
provision
and use of **electronic** information, it is no wonder that the various
players have grown increasingly knowledgeable about the legal
implications

of what they do. Information professionals are not...

...for their professional time and skill. The complex legal issues impact
on information professionals corporately and individually, and, despite the
rhetoric of employee law and **terms** and conditions of use and
disclaimers, there is more and more concern among individual information
professionals that, one day, allegations of professional negligence and
fault will be levelled at them personally. We have seen signs that
responsibility, say for the accuracy of **Web** information or the
careful filtering of a school intranet and the administration of an
acceptable use policy, is likely to be delegated to particular individuals
...

...from a range of factors from direct economic loss and physical injury to
more nebulous but nonetheless tangible things like emotional distress (e.g.
from **electronic** harassment on an e-mail network, exposure to hate
and pornographic text and images on the **Internet** access by school
pupils).

More and more attention is being written about professional conduct where
electronic transactions and communications are concerned. For
example, the ABA/BNA's Lawyers' Manual on Professional Conduct (at the BNA
Website) places emphasis on malpractice and e-mail and **online**
advice. One point is how far can an e-mail correspondence go before it can
be regarded as an attorney-client relationship? This has a...

...message, disclaiming responsibility and liability for inferences clients
might make and uses to which clients might put the information. Often, too,
assertions about intellectual property **rights**, warranties and
endorsements, and privacy and data protection can be made. Commercial
organisations like Jane's and the British Standards Institute, have
foreseen potential difficulties...

...client education, charging, confidentiality and conflicts of interest.
The professional guidelines of the American Society of Information
Scientists picks out privacy and confidentiality, respecting proprietary
rights, providing proper security, not knowingly making false
statements or providing erroneous or misleading information, not
misrepresenting themselves, undertaking research conscientiously in
gathering tabulating or interpreting...

...full compliance with ethical standards within one's company, with
third-party contractors, and within the entire profession.

Ethics encourages us to revisit concepts of **rights**, duties, and
consequences. Duties, in particular, draw on the extensive
deontological
tradition going back to the Ten Commandments, and express themselves
today
in duty-based **books** in school because of majority outrage, select
one system or supplier on pragmatic grounds of cost comparisons and not
on
grounds of loyalty, and elect...

...risk lies in the area of liability, and, at the sharp end when
information professionals are dealing with information and clients,
above
all in the **electronic** domain, that is more a matter of law –
tortious negligence and contractual obligations – than a matter of
ethics.
Moreover, in law, things can be defined in precise **terms**: in tort
the sequence of care and lack of care, fault, reasonableness,
competence,
foreseeability, causation and remoteness, harm or injury, defences and
damages; and in contract law, **terms** and obligations, rationality and
capability, performance and non-performance, breach, defences and
remedies,
damages and compensation.

The emphasis on contractual law, above all, and above all in the field
of
electronic information, points the current way forward in this area
of professional work. Legislation and case law highlight the need to
define
roles and consequences (e.g. of ISPs and sysops, as publishers or
editors
or common carriers). Disclaimers and exclusion clauses, adding to the
contractual **terms** and conditions under which software and hardware
are bought and used, protected and justified, point forward to a sea
change
in professional sentiment. The diffuse...

...Information Age, John Wiley, New York, NY.

3. Connock, S. and Johns, T. (1995), Ethical Leadership, Institute for
Personnel Development, London.

4. Dickie, J. (1999), **Internet** and **Electronic** Commerce Law in
the European Union, Hart Publishing, Oxford.

5. Dragich, M. (1989), "Information malpractice", Information
Technology
and Libraries, Vol. 8 No. 3, pp. 265-72.

6. Dugdale, A.M. and Stanton, K.M. (1989), Professional Negligence,
Butterworths, London.

7. Edwards, L. and Waelde, C. (Eds) (1997), Law and the **Internet**:
Regulating Cyberspace, Hart Publishing, Oxford.

8. Epstein, R. (1997), The Case of the Killer Robot: Stories about the

Professional, Ethical, and Societal Dimensions of Computing...

...2, pp. 91-8.
10. Howarth, D. (1995), Textbook on Tort, Butterworths, London.

11. Hugenholtz, P.B. (Ed.) (1996), The Future of Copyright in a
Digital Environment, Kluwer Law, The Hague.

12. Jackson, R. and Powell, J. (1982), Professional Negligence, Sweet &
Maxwell, London.

13. Kalakota, R. and Whinston, A. (1997), **Electronic** Commerce: A
Manager's Guide, Addison-Wesley, Reading, MA.

14. Lloyd, I. (1993), Information Technology Law, Butterworths, London.

15. Lloyd, I and Simpson, M. (1994), "Law on the **electronic**
frontier", Hume Papers on Public Policy, Vol. 2 No. 4, Edinburgh
University
Press, Edinburgh.

16. Mowatt, M. (1998), Legal Liability for Information Provision,
Aslib,
London.

17. Oppenheim, C. (1999), The Legal and Regulatory Environment for
Electronic Information, 3rd ed., Infonortics Ltd., Tetbury.

18. Perritt, H.H. Jr (1996), Law and the Information Superhighway, John
Wiley, New York, NY.

19. Reed, C. (1996), **Digital** Information Law: **Electronic**
Documents and Requirements of Form, Queen Mary and Westfield College,
Centre for Commercial Law Studies, University of London, London.

20. Rose, L. (1995), Netlaw: Your **Rights** in the **Online** World,
Osborne McGraw-Hill, New York, NY.

21. Sieber, U. (1992), Liability for On-line Banking Services in the
European Community, Carl Heymanns Verlag KG...

Descriptors:
...**Online** information services

Classification Codes:

18/K/3 (Item 1 from file: 16)
DIALOG(R)File 16: Gale Group PROMT(R)

 Supplier Number: (USE FORMAT 7 FOR FULLTEXT)

Using the Web to relieve permissions bottlenecks : Yankee, iCopyright take different tacks to same end.(Yankee Book Peddler)(Company Business and Marketing)

Text:

```
 ...worse as production cycles shrink and the number of titles per
staff increases. This year, two companies with very different
backgrounds
are rolling out similar Web-based services that at least help
alleviate the drudgery on the permission-granting side. Yankee Book
Peddler, an established supplier of bookselling services, and
iCopyright, a
startup, are testing their services this summer in the hopes of
offering
them on a...
```

```
 We'll profile each company and its service, and conclude with a
comparison.
        YBP's Copyright Direct
        Established in 1971, Yankee Book Peddler (YBP) provides
books and supporting collection management and technical services to
academic, research and special libraries in North America and around
the
world. Its electronic services include GOBI, a bibliographic
database.
        The company's headquarters are in New Hampshire; in Europe it is
represented by Lindsay & Howes, which is based in Godalming, outside of
London.
        This past February YBP launched Copyright Direct, an online
service that automates permissions transactions, such as a request to
use a
previously published illustration in a new book or multimedia work.
At that time YBP also announced its first pilot participant, Houghton
Mifflin's College Division.
        Since then, YBP has announced that its academic library services
business will merge with Baker & Taylor. Yankee's Rights
Management Division, including Copyright Direct, was not included and
will
be spun off as a separate company, under the direction of Yankee's
current
CEO...
```

```
...What it provides. For copyright holders, Copyright Direct puts into
place a hands-free way to deal with routine permission requests. Those
seeking permission to license pieces of content submit the request
and, in some cases, even obtain permission directly through the Web
-based system, without having to call, write or fax someone at the
copyright holder. The service saves the rights holder the drudgery
of filling out paperwork on routine permissions, and it can save the
requester processing time.
        How it works. The rights-holding publisher first must load the
Yankee database with a list of the content and the terms of use,
including the price variables. There is a batch-load feature as well as
a
Web interface for changing individual records. If necessary, YBP
```

also works with the publisher to define its database (if its permissions
files are still in file cabinets), customize the system and integrate it
with other **rights**-management software at the publisher. "We view
Copyright Direct as part of an application set for managing **rights**
at the publisher," said Kelly Frey, VP of marketing at YBP. Our software is
an externally visible component, but it may be one of many that a publisher
employs to keep track of how its **content** is **used** and
licensed."

       Once the database is loaded, the permissions staff at the
rights holder uses HTML forms to update their listings on Copyright
Direct. YBP authenticates the staff by user name and password.

       Users (those seeking permission) see a **Web**-based storefront
listing the items that can be **licensed** and providing **online**
forms for buying the **rights** to use specific pieces of content (see
screen shot on p. 22).

       If the publisher allows, the transaction can be completed
online, using YBP's e-commerce system. Otherwise, the request (in a
consistent structured form, with all required fields filled in) is
forwarded to the publisher. Even if the transaction isn't completed
online, Copyright Direct saves the publisher time: the permissions
department receives a well-structured request, with all of the key
variables (publication, length of run, media, etc.) answered.

       Payments may be taken **online** via credit card (Yankee uses
CyberCash to clear the payments). Alternatively, companies can set up
accounts for monthly billing handled by YBP. YBP delivers to the
rights holders monthly payments and activity reports from Copyright
Direct. **Rights** holders can also run payment and activity reports
online in real time by visiting the Copyright Direct **Web**
site.

       Having an account gives you additional features and reporting.

       Pricing. Though it views itself as an integrator, YPB is not charging
an up-front...

...application, which is expected to be live for the public sometime later
this summer from within the permissions portion of the company's College
Division **Web** site (www.hmco.com/college/permissions).

       In its pilot implementation, Houghton Mifflin took the generic
product and has been tailoring it to meet the needs...

...customers, and helps improve compliance with copyright law, we view as a
good thing."

       According to Frey, Copyright Direct might also work for a site
license within a library.

       iCopyright handles **rights**

       In contrast with YBP, which caters to libraries and academic
publishers, iCopyright is a young startup focused on **rights**
management for a broader class of publishers, particularly newspapers and

magazines, who want to reach corporate markets. While not yet operational,
it's currently in...

...and running by the end of the year. Its initial focus will be to provide
an easy-to-use method for corporate accounts to obtain **rights** clearances to commercially published material.

The company was founded by former members of Design Intelligence, makers of iPublish, a desktop publishing tool targeted at non-design professionals that never quite found a market (see Vol. 1, No. 4). One component of that system was a **Web** site for ordering additional clip art **online**. That component was the genesis of iCopyright.

What it provides. Where YBP sells a system that is an extension of
the publisher's permissions department, iCopyright is a **rights** clearinghouse at which a customer can obtain permission from a variety of
publishers. It covers several types of clearances:

* Local. Clearance to print or copy...but this is a contentious area
for publishers. iCopyright can handle this request for those wishing to ensure proper compliance.

* Permission to reuse on the **Web**. Content from a **Web** page can be stripped of banner ads and packaged with relevant graphics. The
item can then be posted to the requestor's **Web** site for a fixed **term.**

The system supports four different classes of users (commercial, non-profit, government, education) with unique fee structures for each. It
also tracks customers individually.

How it works. The iCopyright system operates similarly to YPB's Copyright Direct. The publisher must first register the content with iCopyright and list the available **rights** and appropriate fees. This can be done via a **Web** page or a batch process. The publisher then displays an iCopyright icon next to the content. Clicking on the icon indicates the **licensing rights** that are available and the fees. The user can review a **terms** of use agreement. There are several versions of the agreement depending on the class of users in two
different levels: one written for lay people and one for attorneys. If the
user purchases **rights**, the content is delivered in the correct format; for example, HTML for a **Web** page or sent by FTP to Kinko's for a high quality reprint.

Content is not encrypted by iCopyright; once delivered, its usage cannot be metered or tracked by the publisher. However, for those worried
about **redistribution, content** may be watermarked or coded with a unique serial number that is placed in the output file for identification. Third-party identification systems, such as DOI, are also
supported in addition to iCopyright's **licensing** codes.

Pricing. iCopyright will be selling a service, not a system, and it
does not intend to charge a transaction fee to **rights** buyers.

However, it is asking a 30% commission on the fees customers pay.
Publishers may decide to just raise the price a bit to cover...

...Newsweek), Dow Jones (stories from the Wall Street Journal
Interactive
and Barron's) and the Software & Information Industry Association
(Upgrade magazine and white papers). These **rights** holders will be
testing the service with selected corporate accounts.
        Our take
        Though the services are similar, these two companies are
marketing
them in different ways, and no doubt will appeal to different
customers.
Yankee **Book** Peddler is selling a service that commercial publishers
will offer at their site and integrate with their own **rights**
management software. Over time, it's also likely that YBP will add
features
particular to the university market that it serves.
        In contrast, iCopyright is positioning itself as "the copyright
clearinghouse for the **Web**," calling to mind a head-to-head
competition with Copyright Clearance Center, which also handles
corporate
accounts. To this audience, iCopyright promises to offer a **Web**
-savvy, pleasant user interface and streamlined, operator-free
operation.
Its target markets are likely to appreciate these features.
        The problem facing everyone concerned with **rights** and
permissions is getting the public's attention and convincing it that
intellectual property **rights** are as important as physical property
rights. Technology can ease the path to acquiring permission to
reuse content, but it can't create the desire to comply with
the law when no one seems to be looking.

Company Names:
*Yankee **Book** Peddler; iCopyright Inc.

Descriptors:

Product Names:
*4811528   (**Online** Business Information Services)

Industry Names:

19990701

18/K/4 (Item 1 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB
(c) 2009 Gale/Cengage. All rights reserved.

Making Smart Licensing Decisions.

Text:

 Collection development used to be easy. You bought a **book** or a
subscription, you owned the resource, and access, for the most part,
was
unlimited. The collection was a tangible entity limited only by
space...

 Today's incredible selection of networked **electronic** resources
extends our collections far beyond the physical boundaries of the
library.
But unlike purchasing a **book** where ownership and access are
tangible, access to **digital** resources often takes place within the
confines of a **license** that defines appropriate use over a specified
period of time. Ownership and access are more nebulous and are often
bound
by agreed-upon **terms** negotiated between the licensee (buyer) and the
licensor (vendor). Less-tangible resources and more complicated rules
definitely have implications for negotiating access and managing
content.
        Buying access to a **digital** resource has forever changed the
activity of collection development, and has required us to become
sophisticated negotiators who are adept at reading complicated
licensing agreements and evaluating **digital** products.
Managing these **digital** resources is complicated, but it is possible
if you apply formal evaluation criteria to every product you consider.
Because of my limited space, I'll...

...the decision-making process for content.
        e.val.u.ate--to determine or set the value or amount of; appraise
        Criteria for evaluating today's **digital** resources are not too
different from the criteria first established by Katz in his **book**
Introduction to Reference Work. (1) If we expand on Katz's original
evaluative criteria of "purpose, authority, scope, audience, cost, and
format," this will help us to evaluate **digital** resources with
clarity and depth.
        How well it fits: The products you consider should fit the
collection's current subject scope and depth as defined by the
collection
development policy of your library. Although **digital** resources may
greatly expand the pool of resources you can choose from, the
acquisition
choices you make shouldn't stray from this formal set of...

...and it should be provided in manageable, digestible chunks. Is
subject
coverage deep in some areas, but light in others? If you're evaluating
an
online textbook or journal, is the content offered in full text,
abstracts, or bare-bones tables of contents? Is the **electronic** copy
the same as the print equivalent, and is there a price break to acquire
both? Does the product bundle other resources that you don...

...or that are redundant to your print collection, but that you pay for
anyway? Some content aggregators offer a more a la carte approach to

licensing resources within a specific subject area. Does the product
offer **online** tutorials, help screens, or documentation for both
systems/product management, as well as end-user training? Does the
product
offer value-added features such as...

...usually quite specific about what constitutes fair use. In some
instances users are allowed to download or print content for personal
use,
but may not **redistribute content** in **electronic** format,
e.g., on a listserv or bulletin board. Pay close attention to your
license agreement, since fair use is defined differently in the
electronic world than in the print world. This could have bearing on
interlibrary loan, reserves, and other educational uses.
        Formatting: If downloading is permissible, can it...

...a bear to maintain, especially when you start to hear daily
complaints
about it from equally frustrated patrons only a month into a year-long
license.
        From a user's perspective, a well-designed product is intuitive
to
use and easy to navigate. It should support a variety of
information-seeking...

...product should be stable without major redesigns occuring for no
apparent reason. Within reason, the product should work regardless of
browser type or version (Netscape, **Internet** Explorer, America
Online, etc. version 3.0 or higher), platform (PC and Mac), and
monitor resolution.
        Access: Some of the most challenging aspects of **licensing**
electronic resources are issues concerning access. Most
licensed resources require some type of procedure to ensure
"appropriate use." Appropriate use is determined by the agreed-upon
terms of the **license** and is carried out through an
identification/authentication protocol. Identification tells the system
that controls access who you are; authentication proves it. These two
steps
secure content by restricting access. The combination of
identification/authentication can be carried out with login/password,
IP
range restrictions, or newer technology such as **digital**
certificates, ...dynamic password, and PIN. Security for content
should be
appropriate, and the administration workload (password resets, etc.)
needs
to be considered, if security mechanisms are **used** to implement
content restrictions, what are the implications both for end-users
and for management?
        Evaluating the vendor: Before you purchase access to a **digital**
resource, know something about the vendor. How long has the company
been in
business? What's the current version of the product you're
considering...

...the vendor to refer you to other similar institutions that have

purchased the product, and try to find formal reviews. Given today's very
competitive **online** content market, what's the vendor's current
financial situation? Is the company stable? Is the vendor in the market
mainstream--that is, does it...

...those you serve, if R&D efforts don't make sense, reconsider your
vendor options.

ne.go.ti.ate--mutual discussion and arrangement of the **terms**
of a transaction or agreement

Licensing electronic resources offers unique challenges
that cannot be resolved by applying the same rules that govern our
acquisition of traditional print resources. Chief among these are
issues of
ownership and access. A **licensed electronic** resource requires
that the vendor give permission to the library (licensee) to distribute
and
make available specific content for an agreed-upon duration and cost.
The
terms also specifically address how the content may/may not be used
(fair use), how the content may be accessed (within the library or
remotely), and who is defined as a "user" (authorized and
unauthorized).

Licensing agreements can be complicated to read unless you
understand the legal and technical jargon used to define the **terms.**
You can find a thorough treatment of this vocabulary at the Lib
License Web site (http://www.library.yale.edu/(sim)llicense),
from Yale University Library, along with other useful **licensing**
information. The Association of Research Libraries also has prepared a
comprehensive guide entitled "Principles for **Licensing
Electronic** Resources" (http://www.arl.org/scomm/**licensing**
/principles.html). I recommend both resources for anyone who is
preparing
to negotiate a **license** or evaluate a product.

Once you're versed in the language of **licensing,** consider
creating a **licensing** template that lists **terms** you can agree
with. Most **license** agreements share a consistent framework of
clauses. Use a standard **license** agreement to craft your own, and
develop a checklist of manageable **terms** and conditions that
adequately serves your users, but that your staff can manage.

Below I've included the main points from a useful checklist
developed
by the European Copyright User Platform. (2)

Don't sign a **license** that (ldots)
* isn't governed by the law and courts of the country where your
institution is located.
* doesn't recognize the statutory **rights** for usage under
copyright.
* doesn't grant perpetual access to the **licensed** material.
* doesn't include a warranty for IP **rights** and an indemnity
clause against claims.
* holds the library liable for each and every infringement by an
authorized user.
* has a non-cancellation clause.
* has...

...has reasonable and best-effort clauses.

* has clauses with ambiguous periods of time.
        * doesn't allow for subcontracting to an agent.
        * hasn't got a **license** fee that is all inclusive.
        man.age--to handle, direct, govern, or control in action or use
        The ability to manage the **licensed electronic** resource
is an important consideration when you evaluate a product. How will the
resource be managed both as a stand-alone resource and as a piece of
your
larger **digital** collection? Increasingly, a library's **Web** site
is the main point of entry into its collections, both **digital** and
print. Our challenge as librarians and developers of front-end gateways
to
these resources is to seamlessly integrate the different products and
resources that make up the collection so users can browse much as they
would **books** on a shelf.
        This isn't an easy task. Just like **books** have different
covers, **digital** resources have different interfaces. Where
traditional print materials like **books** and journals have consistent
structures (table of contents, chapters, appendixes, and index),
digital resources often lack these perceptible cues that help users
navigate the content. In addition, not all content we purchase is
accessible from a browser session...

...users all these incredible resources without confusing them at the
same
time?
        Consider these criteria when assessing the manageability of a
product:
        * Where will the **licensed** product or content physically
reside--the library's server or the vendor's?
        * Does the vendor offer trial access to its product?
        * Who is responsible...

...will users want to access this resource, e.g., using PCs within the
library, using PCs with remote dial-up, using other devices like
personal
digital assistants (PDAs)?
        * Can this product be integrated easily into existing products or
environments such as the library's **online** catalog, **Web** page,
or portal?
        * Is the authentication procedure itself a barrier to entry?
        * What usage data can be expected from the vendor and in what
format
...given by the vendor (24/7 or 9-to-5, 5 days a week)?
        As you apply your own formal set of evaluative criteria for
licensing digital resources, you'll find that the process
gets easier. You'll recognize good products when you see them and
you'll
stay clear of those that don't meet your high standards. You'll be able
to
recognize **license terms** that don't make sense or that are
worth negotiating. In the end, the actual process of evaluation will
ultimately help you manage your **digital** collections more
efficiently.
        As **digital** librarians, we are in an environment with a rich
selection of **electronic** resources. We can easily flood library

patrons with information or confuse them with obstacles of
authentication
protocols, interface designs, and search engines, so we must choose
well.
Digital resources are less tangible, are more complex in
terms of content and implementation, require more skills to procure
and manage, and most surely show us what our future is all about.
Deciding
how we guide patrons into this **digital** future will be the challenge.
    Kim Guenther is the **Internet**/clinical information services
coordinator for the University of Virginia Health Sciences Library and
UVa
Health System Webmaster.
    References
    (1.) Katz, William A. Introduction to Reference Work. New York:
McGraw-Hill, 1992.
    (2.) **"Licensing Digital** Resources: How to avoid the
legal pitfalls?" European Copyright User Platform, Netherlands,
November 9,
1998 (http://www.eblida.org/ecup/docs).
    Further Reading
    Brennan, Patricia; Hersey, Karen; and Harper, Georgia. "
Licensing Electronic Resources: Strategic and Practical
Considerations for Signing **Electronic** Information Delivery
Agreements" (http://www.arl.org/scomm/**licensing**/licbookler.html).
    "Principles for **Licensing Electronic** Resources," (final
draft) July 15, 1997 (http://www.arl.org/scomm/**licensing**
/principles.html).
    International Coalition of Library Consortia
(http://www.library.yale.edu/consonia).
    Soete, George J. "Managing the **Licensing** of **Electronic**
Products," Washington, DC: Association of Research Libraries, Office of
Leadership and Management Services, 1999
(http://www.arl.org/olms/infosvcs.html).

20000601

18/K/5 (Item 1 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)
(c) 2009 Gale/Cengage. All rights reserved.

Making Smart Licensing Decisions.(Industry Trend or Event)

Text:
 Collection development used to be easy. You bought a book or a
subscription, you owned the resource, and access, for the most part,
was
unlimited. The collection was a tangible entity limited only by
space...

 Today's incredible selection of networked electronic resources

extends our collections far beyond the physical boundaries of the
library.
But unlike purchasing a book where ownership and access are
tangible, access to digital resources often takes place within the
confines of a license that defines appropriate use over a specified
period of time. Ownership and access are more nebulous and are often
bound
by agreed-upon terms negotiated between the licensee (buyer) and the
licensor (vendor). Less-tangible resources and more complicated rules
definitely have implications for negotiating access and managing
content.
        Buying access to a digital resource has forever changed the
activity of collection development, and has required us to become
sophisticated negotiators who are adept at reading complicated
licensing agreements and evaluating digital products.
Managing these digital resources is complicated, but it is possible
if you apply formal evaluation criteria to every product you consider.
Because of my limited space, I'll...

...the decision-making process for content.
        e.val.u.ate--to determine or set the value or amount of; appraise
        Criteria for evaluating today's digital resources are not too
different from the criteria first established by Katz in his book
Introduction to Reference Work. (1) If we expand on Katz's original
evaluative criteria of "purpose, authority, scope, audience, cost, and
format," this will help us to evaluate digital resources with
clarity and depth.
        How well it fits: The products you consider should fit the
collection's current subject scope and depth as defined by the
collection
development policy of your library. Although digital resources may
greatly expand the pool of resources you can choose from, the
acquisition
choices you make shouldn't stray from this formal set of...

...and it should be provided in manageable, digestible chunks. Is
subject
coverage deep in some areas, but light in others? If you're evaluating
an
online textbook or journal, is the content offered in full text,
abstracts, or bare-bones tables of contents? Is the electronic copy
the same as the print equivalent, and is there a price break to acquire
both? Does the product bundle other resources that you don...

...or that are redundant to your print collection, but that you pay for
anyway? Some content aggregators offer a more a la carte approach to
licensing resources within a specific subject area. Does the product
offer online tutorials, help screens, or documentation for both
systems/product management, as well as end-user training? Does the
product
offer value-added features such as...

...usually quite specific about what constitutes fair use. In some
instances users are allowed to download or print content for personal
use,
but may not redistribute content in electronic format,
e.g., on a listserv or bulletin board. Pay close attention to your

license agreement, since fair use is defined differently in the
electronic world than in the print world. This could have bearing on
interlibrary loan, reserves, and other educational uses.
  Formatting: If downloading is permissible, can it...

...a bear to maintain, especially when you start to hear daily
complaints
about it from equally frustrated patrons only a month into a year-long
license.
  From a user's perspective, a well-designed product is intuitive
to
use and easy to navigate. It should support a variety of
information-seeking...

...product should be stable without major redesigns occuring for no
apparent reason. Within reason, the product should work regardless of
browser type or version (Netscape, Internet Explorer, America
Online, etc. version 3.0 or higher), platform (PC and Mac), and
monitor resolution.
  Access: Some of the most challenging aspects of licensing
electronic resources are issues concerning access. Most
licensed resources require some type of procedure to ensure
"appropriate use." Appropriate use is determined by the agreed-upon
terms of the license and is carried out through an
identification/authentication protocol. Identification tells the system
that controls access who you are; authentication proves it. These two
steps
secure content by restricting access. The combination of
identification/authentication can be carried out with login/password,
IP
range restrictions, or newer technology such as digital
certificates, ...dynamic password, and PIN. Security for content
should be
appropriate, and the administration workload (password resets, etc.)
needs
to be considered, if security mechanisms are used to implement
content restrictions, what are the implications both for end-users
and for management?
  Evaluating the vendor: Before you purchase access to a digital
resource, know something about the vendor. How long has the company
been in
business? What's the current version of the product you're
considering...

...the vendor to refer you to other similar institutions that have
purchased the product, and try to find formal reviews. Given today's
very
competitive online content market, what's the vendor's current
financial situation? Is the company stable? Is the vendor in the market
mainstream--that is, does it...

...those you serve, if R&D efforts don't make sense, reconsider your
vendor options.
  ne.go.ti.ate--mutual discussion and arrangement of the terms
of a transaction or agreement
  Licensing electronic resources offers unique challenges
that cannot be resolved by applying the same rules that govern our

acquisition of traditional print resources. Chief among these are issues of
ownership and access. A licensed electronic resource requires
that the vendor give permission to the library (licensee) to distribute and
make available specific content for an agreed-upon duration and cost. The
terms also specifically address how the content may/may not be used
(fair use), how the content may be accessed (within the library or
remotely), and who is defined as a "user" (authorized and unauthorized).

Licensing agreements can be complicated to read unless you
understand the legal and technical jargon used to define the terms.
You can find a thorough treatment of this vocabulary at the Lib
License Web site (http://www.library.yale.edu/(sim)llicense),
from Yale University Library, along with other useful licensing
information. The Association of Research Libraries also has prepared a
comprehensive guide entitled "Principles for Licensing
Electronic Resources" (http://www.arl.org/scomm/licensing
/principles.html). I recommend both resources for anyone who is preparing
to negotiate a license or evaluate a product.

Once you're versed in the language of licensing, consider
creating a licensing template that lists terms you can agree
with. Most license agreements share a consistent framework of
clauses. Use a standard license agreement to craft your own, and
develop a checklist of manageable terms and conditions that
adequately serves your users, but that your staff can manage.

Below I've included the main points from a useful checklist developed
by the European Copyright User Platform. (2)

Don't sign a license that (ldots)

* isn't governed by the law and courts of the country where your institution is located.
* doesn't recognize the statutory rights for usage under copyright.
* doesn't grant perpetual access to the licensed material.
* doesn't include a warranty for IP rights and an indemnity clause against claims.
* holds the library liable for each and every infringement by an authorized user.
* has a non-cancellation clause.
* has...

...has reasonable and best-effort clauses.
* has clauses with ambiguous periods of time.
* doesn't allow for subcontracting to an agent.
* hasn't got a license fee that is all inclusive.
man.age--to handle, direct, govern, or control in action or use
The ability to manage the licensed electronic resource
is an important consideration when you evaluate a product. How will the
resource be managed both as a stand-alone resource and as a piece of your
larger digital collection? Increasingly, a library's Web site
is the main point of entry into its collections, both digital and
print. Our challenge as librarians and developers of front-end gateways to

these resources is to seamlessly integrate the different products and
resources that make up the collection so users can browse much as they
would books on a shelf.

This isn't an easy task. Just like books have different
covers, digital resources have different interfaces. Where
traditional print materials like books and journals have consistent
structures (table of contents, chapters, appendixes, and index),
digital resources often lack these perceptible cues that help users
navigate the content. In addition, not all content we purchase is
accessible from a browser session...

...users all these incredible resources without confusing them at the
same
time?

Consider these criteria when assessing the manageability of a
product:

    * Where will the licensed product or content physically
reside--the library's server or the vendor's?
    * Does the vendor offer trial access to its product?
    * Who is responsible...

...will users want to access this resource, e.g., using PCs within the
library, using PCs with remote dial-up, using other devices like
personal
digital assistants (PDAs)?
    * Can this product be integrated easily into existing products or
environments such as the library's online catalog, Web page,
or portal?
    * Is the authentication procedure itself a barrier to entry?
    * What usage data can be expected from the vendor and in what
format
...given by the vendor (24/7 or 9-to-5, 5 days a week)?

As you apply your own formal set of evaluative criteria for
licensing digital resources, you'll find that the process
gets easier. You'll recognize good products when you see them and
you'll
stay clear of those that don't meet your high standards. You'll be able
to
recognize license terms that don't make sense or that are
worth negotiating. In the end, the actual process of evaluation will
ultimately help you manage your digital collections more
efficiently.

As digital librarians, we are in an environment with a rich
selection of electronic resources. We can easily flood library
patrons with information or confuse them with obstacles of
authentication
protocols, interface designs, and search engines, so we must choose
well.
Digital resources are less tangible, are more complex in
terms of content and implementation, require more skills to procure
and manage, and most surely show us what our future is all about.
Deciding
how we guide patrons into this digital future will be the challenge.

Kim Guenther is the Internet/clinical information services
coordinator for the University of Virginia Health Sciences Library and
UVa
Health System Webmaster.

        References
        (1.) Katz, William A. Introduction to Reference Work. New York:
McGraw-Hill, 1992.
        (2.) "Licensing Digital Resources: How to avoid the
legal pitfalls?" European Copyright User Platform, Netherlands,
November 9,
1998 (http://www.eblida.org/ecup/docs).
        Further Reading
        Brennan, Patricia; Hersey, Karen; and Harper, Georgia. "
Licensing Electronic Resources: Strategic and Practical
Considerations for Signing Electronic Information Delivery
Agreements" (http://www.arl.org/scomm/licensing/licbookler.html).
        "Principles for Licensing Electronic Resources," (final
draft) July 15, 1997 (http://www.arl.org/scomm/licensing
/principles.html).
        International Coalition of Library Consortia
(http://www.library.yale.edu/consonia).
        Soete, George J. "Managing the Licensing of Electronic
Products," Washington, DC: Association of Research Libraries, Office of
Leadership and Management Services, 1999
(http://www.arl.org/olms/infosvcs.html).

20000601

18/K/6 (Item 1 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

Country	Number	Kind	Date

Legal Status Type	Pub. Date	Kind	Text

Language

Fulltext Availability Available Text	Language	Update	Word Count
Total Word Count (Document A)			
Total Word Count (Document B)			
Total Word Count (All Documents)			

Specification: ...to the downloaded Player Application 195 and that the End-User Device(s) 109 stores it for later application license verification (see below).

The overall **licensing** flow starts at the Content Provider(s) 101. The Content Provider(s) 101 encrypts the Content 113 using an encryption symmetric key locally generated, and...
...Conditions 519 associated with the Content Usage Control Layer 505.

The Content Provider(s) 101 distributes the Metadata SC(s) 620 to one or more **Electronic Digital** Content Store(s) 103 (step601) and the Content SC(s) 630 to one or more Content Hosting Sites (step602). Each **Electronic Digital** Content Store(s) 103, in turn creates an Offer SC(s) 641. The Offer SC(s) 641 typically carries much of the same information as the Metadata SC(s) 620, including the **Digital** Signature 624 of the Content Provider(s) 101 and the Certificate (not shown of the Content Provider(s) 101. As mentioned above, the **Electronic Digital** Content Store(s) 103 can add to or narrow the Store Usage Conditions 519 (handled by the Control Usage Control Layer) initially defined by the Content Provider(s) 101. Optionally, the Content SC(s) 630 and/or the Metadata SC(s) 620 is signed with a **Digital** Signature 624 of the Content Provider(s) 101.

After the completion of the Content-purchase transaction between the End-User Device(s) 109 and the **Electronic Digital** Content Store(s) 103 (step603), the **Electronic Digital** Content Store(s) 103 creates and transfers to the End-User Device(s) 109 a Transaction SC(s) 640 (step604). The Transaction SC(s) 640...Transaction Data 642 is encrypted with the Public Key 621 of the ClearingHouse(s) 105. Optionally, the Transaction SC(s) 640 is signed with a **Digital** Signature 643 of the **Electronic Digital** Content Store(s) 103.

Upon reception of the Transaction SC(s) 640 (and the Offer SC(s) 641 included in it), the End-User Player Application 195 running on End-User Device(s) 109 solicits **license** authorisation from the ClearingHouse(s) 105 by means of an Order SC(s) 650 (step605). The Order SC(s) 650 includes the encrypted Symmetric Key... ...and the encrypted Application ID 551 from the End-User Device(s) 109. In another embodiment, the Order SC(s) 650 is signed with a **Digital** Signature 652 of the End-User Device(s) 109.

Upon reception of the Order SC(s) 650 from the End-User Device(s) 109, the ClearingHouse(s) 105 verifies:

1. that the **Electronic Digital** Content Store(s) 103 has authorisation from the Secure **Digital** Content **Electronic** Distribution System 100 (exists in the Database 160 of the ClearingHouse(s) 105);

2. that the Order SC(s) 650 has not been altered;

3. that the Transaction Data 642 and Symmetric Key 623 are complete and authentic;

4. that the **electronic** Store Usage Conditions 519 purchased by the End-User Device(s) 109 are consistent with those Usage Conditions 517 set by the Content Provider(s) 101; and

5. that the Application ID 551 has a valid structure and that it was provided by an authorised **Electronic Digital** Content Store(s) 103. If the verifications are successful, the ClearingHouse(s) 105 decrypts the Symmetric Key 623 and the Transaction Data 642 and builds and transfers the **License** SC(s) 660 to the End-User Device(s) 109 (step606). The

License SC(s) 660 carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the Public Key 661 of the End-User Device(s) 109. If any verification is not successful, the ClearingHouse(s) 105 denies the **license** to the End-User Device(s) 109 and informs the End-User Device(s) 109. The ClearingHouse(s) 105 also immediately informs the **Electronic Digital** Content Store(s) 103 of this verification failure. In an alternate embodiment, the ClearingHouse(s) 105 signs the **License** SC(s) 660 with its **Digital** Signature 663.

After receiving the **License** SC(s) 660, the End-User Device(s) 109 decrypts the Symmetric Key 623 and the Transaction Data 642 previously received from the ClearingHouse(s... ...decrypts the Content 113 using the Symmetric Key 623 (step609), and passes the Content 113 and the Transaction Data 642 to the other layers for **license** Watermarking, copy/play coding, scrambling, and further Content 113 processing as described previously for FIG. 5.

Finally, the ClearingHouse(s) 105 on a periodic basis transmits summary transaction reports to the Content Provider(s) 101 and the **Electronic Digital** Content Store(s) 103 for auditing and tracking purposes (step610).

V. SECURE CONTAINER STRUCTURE

A. General Structure

A Secure Container (SC) is a structure that... ...together and another digest is computed from them and then encrypted using the private key of the entity creating the SC(s) to create a **digital** signature. Parties receiving the SC(s) can use the **digital** signature to verify all of the digests and thus validate the integrity and completeness of the SC(s) and all of its parts.

The following... ...records need to be included:

* SC(s) version

* SC(s) ID

* Type of SC(s) (e.g. Offer, Order, Transaction, Content, Metadata or promotional and **License**.)

* Publisher of the SC(s)

* Date that the SC(s) was created

* Expiration date of the SC(s)

* ClearingHouse(s) URL

* Description of the digest algorithm used for the included parts(default is MD-5)

*Description of the algorithm used for the **digital** signature encryption (default is RSA)

* **Digital** signature (encrypted digest of all of the concatenated digests of the included parts)

SC(s) may include more than one BOM. For example, an Offer SC(s) 641 consists of the original Metadata SC(s) 620 parts, including its BOM, as well as additional information added by the **Electronic Digital** Content Store(s) 103 and a new BOM. A record for the Metadata SC(s) 620 BOM is included in the Offer SC(s) 641...the Metadata SC(s) 620 have records in the new BOM that was created for the Offer SC(s) 641. Only parts added by the **Electronic Digital** Content Store(s) 103 and the Metadata SC(s) 620 BOM have records in the new BOM.

SC(s) may also include a Key Description... ...was used to encrypt the encrypted part.

If the SC(s) does not contain any encrypted parts, then there is no Key Description part.

B. **Rights** Management Language Syntax and Semantics

The **Rights** Management Language consists of parameters that can be assigned values to define restrictions on the use of the Content 113 by an End-User(s... ...the Content 113 is the Usage Conditions 517. Each Content Provider(s) 101 specifies the Usage Conditions 517 for each of its Content 113 items. **Electronic Digital** Content Store(s) 103 interpret the Usage Conditions 517 in Metadata SC(s) 620 and use the information to provide select options they wish to... ...the End-User Device(s) 109 requests authorisation for the Content 113 based on Store Usage Conditions 519. Before the ClearingHouse(s) 105 sends a **License** SC(s) 660 to the End-User(s), the ClearingHouse(s) 105 verifies that the Store Usage Conditions 519 being requested are in agreement with... ...were encoded into the Content 113 are enforced.

The following are examples of Store Usage Conditions 519 for an embodiment where the Content 113 is **music**:

* Song is recordable.

* Song can be played n number of times.

C. Overview of Secure Container Flow and Processing

Metadata SC(s) 620 are built by Content Provider(s) 101 and are **used** to define **Content** 113 items such as songs. The Content 113 itself is not included in these SC(s) because the size of the Content 113 is typically too large for **Electronic Digital** Content Store(s) 103 and End-User(s) to efficiently download the containers just for the purpose of accessing the descriptive metadata. Instead, the SC... ...the Content 113. The SC(s) also includes metadata that provides descriptive information about the Content 113 and any other associated data, such as for **music**, the CD cover art and/or **digital audio** clips in the case of song Content 113.

Electronic Digital Content Store(s) 103 download the Metadata SC(s) 620, for which they are authorised, and build Offer SC(s) 641. In short, an Offer SC(s) 641 consists of some of the parts and the BOM from the Metadata SC(s) 620 along with additional information included by the **Electronic Digital** Content Store(s) 103. A new BOM for the Offer SC(s) 641 is created when the Offer SC(s) 641 is built. **Electronic Digital** Content Store(s) 103 also use the Metadata SC(s) 620 by extracting metadata information from them to build HTML pages on their **web** sites that present descriptions of Content 113 to End-User(s), usually so they can purchase the Content 113.

The information in the Offer SC(s) 641 that is added by the **Electronic Digital** Content Store(s) 103 is typically to narrow the selection of Usage Conditions 517 that are specified in the Metadata SC(s) 620 and promotional data such as a graphic image file of the store's logo and a URL to the store's **web** site. An Offer SC(s) 641 template in the Metadata SC(s) 620 indicates which information can be overridden by the **Electronic Digital** Content Store(s) 103 in the Offer SC(s) 641 and what, if any, additional information is required by the **Electronic Digital** Content Store(s) 103 and what parts are retained in the embedded Metadata SC(s) 620.

Offer SC(s) 641 are included in a Transaction SC(s) 640 when an End-User(s) decides to purchase Content 113 from an **Electronic Digital** Content Store(s) 103. The **Electronic Digital** Content Store(s) 103 builds a Transaction SC(s) 640 and includes Offer SC(s) 641 for each Content 113 item being purchased and transmits...ClearingHouse(s) 105 validates and processes Order SC(s) 650 to provide the End-User Device(s) 109 with everything that is required to a **License** Watermark 527 and access purchased Content 113. One of the functions of the ClearingHouse(s) 105 is to decrypt the Symmetric Keys 623 that are... ...the SC(s) and encrypts them again with the Public Key 661 of the End-User Device(s) 109. The ClearingHouse(s) 105 builds a **License** SC(s) 660 that includes the newly encrypted Symmetric Keys 623 and updated watermarking instructions and sends it to the End-User Device(s) 109... ...the ClearingHouse(s) 105 returns to the End-User Device(s) 109 an HTML page or equivalent reporting the failure of the authorisation process.

A **License** SC(s) 660 provides an End-User Device(s) 109 with everything that is needed to access a Content 113 item. The End-User Device... ...Content Provider(s) 101 and include encrypted Content 113 and metadata parts. The End-User Player Application 195

uses the Symmetric Keys 623 from the **License** SC(s) 660 to decrypt the Content 113, metadata, and watermarking instructions. The watermarking instructions are then affixed into the Content 113 and the Content... ...template), although the entire original BOM is propagated. This is done because the entire BOM is required by the ClearingHouse(s) 105 to verify the **digital** signature in the original SC(s).

The Key Description Part columns of the following table define the records that are included in the Key Description... ...was used to encrypt the Symmetric Key 623 when the Key Id/Enc Key column is an encrypted Symmetric Key 623.

The following describes the **terms** that are used in the above Metadata SC(s) table:

* (Content URL) - A parameter in a record in the Key Description part. This is a...use of the Content 113.

* SC(s) Templates - Parts that define templates that describe the required and optional information for building the Offer, Order, and **License** SC(s) 660.

* Watermarking Instructions - A part that contains the encrypted instructions and parameters for implementing watermarking in the Content 113. The watermarking instructions may be modified by the ClearingHouse(s) 105 and returned back to the End-User Device(s) 109 within the **License** SC(s) 660. There is a record in the Key Description part that defines the encryption algorithm that was used to encrypt the watermarking instructions... ...obtain the proper authorisation to access the Content 113.

* Digest Algorithm ID - An identifier of the algorithm used to compute the digests of the parts.

* **Digital** Signature Alg ID - An identifier of the algorithm used to encrypt the digest of the concatenated part digests. This encrypted value is the **digital** signature.

* **Digital** Signature - A digest of the concatenated part digests encrypted with the public key of the entity that created the SC(s).

* Output Part - The name... ...of the metadata parts, and BOM from the Metadata Sc(s) 620 are also included in the Offer SC(s) 641.

The following describes the **terms** that are used in the above Offer SC(s) 641 that were not previously described for another SC(s):

* Metadata SC(s) BOM - The BOM... ...s) 641 BOM includes the digest of the Metadata SC(s) 620 BOM.

* Additional and Overridden Fields - Usage conditions information that was overridden by the **Electronic Digital** Content Store(s) 103. This information is validated by the ClearingHouse(s) 105, by means of the received SC(s) templates, to make sure that

anything that the **Electronic Digital** Content Store(s) 103 overrides is within the scope of its authorisation.

* **Electronic Digital** Content Store(s) Certificate - A certificate provided to the **Electronic Digital** Content Store(s) 103 by the ClearingHouse(s) 105 and signed by the ClearingHouse(s) 105 using its private key. This certificate is used by the End-User Player Application 195 to verify that the **Electronic Digital** Content Store(s) 103 is a valid distributor of Content 113. The End-User Player Application 195 and ClearingHouse(s) 105 can verify that the **Electronic Digital** Content Store(s) 103 is an authorised distributor by decrypting the certificate's signature with the Clearinghouse's 105 Public Key 621. The End-User...shows the parts that are included in the Transaction SC(s) 640 as well as its BOM and Key Description parts.

The following describes the **terms** that are used in the above Transaction SC(s) 640 that were not previously described for another SC(s):

* Transaction ID 535 - An ID assigned by the **Electronic Digital** Content Store(s) 103 to uniquely identify the transaction.

* End-User(s) ID - An identification of the End-User(s) obtained by the **Electronic Digital** Content Store(s) 103 at the time the End-User(s) makes the buying selection and provides the credit card information.

* End-User(s)' Public... ...is used by the ClearingHouse(s) 105 to re-encrypt the Symmetric Keys 623. The End-User(s)' Public Key 661 is transmitted to the **Electronic Digital** Content Store(s) 103 during the purchase transaction.

* Offer SC(s) - Offer SC(s) 641 for the Content 113 items that were purchased.

* Selections of... ...entry for each Offer SC(s) 641.

* HTML to Display - One or more HTML pages that the End-User Player Application 195 displays in the **Internet** browser window upon receipt of the Transaction SC(s) 640 or during the interaction between the End-User Device(s) 109 and the ClearingHouse(s... ...SC(s) 640, the following steps may be performed to verify the integrity and authenticity of the SC(s):

1. Verify the integrity of the **Electronic Digital** Content Store(s) 103 certificate using the Public Key 621 of the ClearingHouse(s) 105. The Public Key 621 of the ClearingHouse(s) 105 was... ...s) 109 after it was received as part of the initialisation of the End-User Player Application 195 during its installation process.

2. Verify the **Digital** Signature 643 of the SC(s) using the public key from the **Electronic Digital** Content Store(s) 103 certificate.

3. Verify the hashes of the SC(s) parts.

4. Verify the integrity and authenticity of each Offer SC(s... ...any change so that the ClearingHouse(s) 105 can validate the integrity of the Metadata SC(s) 620 and its parts. The following describes the **terms** that are used in the above Order SC(s) 650 that were not previously described for another SC(s):

* Transaction SC(s) BOM - The BOM... ...from the End-User(s) that is used to charge the purchase to a credit card or * debit card. This information is required when the **Electronic Digital** Content Store(s) 103 that created the Offer SC(s) 641 does not handle the customer billing, in which case the ClearingHouse(s) 105 may handle the billing.

H. **License** Secure Container 660 Format

The following table shows the parts that are included in the **License** SC(s) 660 as well as its BOM. As shown in the Key Description part, the Symmetric Keys 623 that are required for decrypting the... ...been re-encrypted by the ClearingHouse(s) 105 using the End-User(s)' Public Key 661. When the End-User Device(s) 109 receives the **License** SC(s) 660 it decrypts the Symmetric Keys 623 and use them to access the encrypted parts from the **License** SC(s) 660 and the Content SC(s) 630.

The following describes the **terms** that are used in the above **License** SC(s) 660 that were not previously described for another SC(s):

* EU Pub Key - An identifier that indicates that the End-User(s)' Public... ...Format

The following table shows the parts that are included in the Content SC(s) 630 as well as the BOM:

The following describes the **terms** used in the above Content SC(s) 630 that were not previously described for another SC(s):

* Encrypted Content - Content 113 that was ...There is no Key Description part included in the Content SC(s) 630 since the keys required to decrypt the encrypted parts are in the **License** SC(s) 660 that is built at the ClearingHouse(s) 105.

VI. SECURE CONTAINER PACKING AND UNPACKING

A. Overview

The SC(s) Packer is a... ...specified parts. The SC(s) Packer 151, 152, 153 variety of hardware platforms supporting Windows' program at the Content Provider(s) 101,

ClearingHouse(s) 105, **Electronic Digital** Content Store(s) 103 and other sites requiring SC(s) Packing. A BOM and, if necessary, a Key Description part are created and included in... ...Description parts and to include parts in the SC(s). Encryption of parts and Symmetric Keys 623 as well as computing the digests and the **digital** signature is also be performed by the packer. Encryption and digest algorithms that are supported by the packer are included in the packer code or... ...processed. Bundling the parts into a single object is the last step that is performed when building a SC(s).

- Indication as to whether the **digital** signature is omitted from the BOM part. If this flag is not set, then the **digital** signature is computed **right** before the SC(s) is bundled into a single object.

In an alternate embodiment, the interface to the packer for building a SC(s) is... ...on a single line with a new line indicating the start of a new record.

The BOM usually includes digests for each part and a **digital** signature that can be used to validate the authenticity and integrity of the SC(s).

The record types within a BOM are as follows:

IP...Description part.

W part(underscore)name (digest)

Specifies the watermarking instructions part.

C part(underscore)name (digest)

Specifies the certificate(s) used to validate the **digital** signature.

T part(underscore)name (digest)

Specifies the Usage Conditions part.

YF part(underscore)name (digest)

Specifies the Template part for the Offer SC(s... ...YO part(underscore)name (digest)

Specifies the Template part for the Order SC(s) 650.

YL part name (digest)

Specifies the Template part for the **License** SC(s) 660.

ID part(underscore)name (digest)

Specifies the ID(s) of the Content 113 of the item(s) of Content 113 being referenced.

CH part(underscore)name (digest)

Specifies the ClearingHouse(s) 105 certificate part.

SP part(underscore)name (digest) Specifies the **Electronic Digital** Content Store(s) 103 certificate part.

B part(underscore)name (digest)

Specifies a BOM part for another SC(s) that has its parts or a... ...underscore)name (digest)

Specifies a data (or metadata) part.

S

An S record is a signature record the is used to define the **digital** signature of the SC(s). The **digital** signature is specified as follows:

S key(underscore)identifier signature(underscore)string signature(underscore)algorithm

The S record contains the key(underscore)identifier to indicate the encryption key of the signature, the signature(underscore)string, which is the base64 encoding of the **digital** signature bitstring, and the signature algorithm that was used to encrypt the digest to create the **digital** signature.

C. Key Description Part

The Key Description part is created by the packer to provide information about encryption keys that are needed for...Key 623 bit string that was used to encrypt the part.

VII. CLEARINGHOUSE(S) 105

A. Overview

The ClearingHouse(s) 105 is responsible for the **rights** management functions of the Secure **Digital** Content **Electronic** Distribution System 100. ClearingHouse(s) 105 functions include enablement of **Electronic Digital** Content Store(s) 103, verification of **rights** to Content 113, integrity and authenticity validation of the buying transaction and related information, distribution of Content encryption keys or Symmetric Keys 623 to End-User Device(s) 109, tracking the distribution of those keys, and reporting of transaction summaries to **Electronic Digital** Content Store(s) 103 and Content Provider(s) 101. Content encryption keys are used by End-User Device(s) 109 to unlock Content 113 for which they have obtained **rights**, typically by a purchase transaction from an authorised **Electronic Digital** Content Store(s) 103. Before a Content encryption key is sent to an End-User Device(s) 109, the ClearingHouse(s) 105 goes through a verification process to validate the authenticity of the entity that is selling the Content 113 and the **rights** that the End-User Device(s) 109 has to the Content 113. This is called the SC Analysis Tool 185. In some configurations the ClearingHouse(s) 105 may also handle the financial settlement of Content 113 purchases by co-locating a system at the ClearingHouse(s) 105 that performs the **Electronic Digital** Content Store(s) 103 functions of credit card authorisation and billing. The ClearingHouse(s) 105 uses OEM packages such as ICVerify and Taxware to handle the credit card processing and local sales taxes.

Electronic Digital Content Store(s) Embodiment

An **Electronic Digital** Content Store(s) 103 that wants to participate as a seller of Content 113 in the Secure **Digital** Content **Electronic** Distribution System 100 makes a request to one or more of the **Digital** Content Provider(s) 101 that provide Content 113 to the Secure **Digital** Content **Electronic** Distribution System 100. There is no definitive process for making the request so long as the

two parties come to an agreement. After the **digital** content label such as a **Music Label** e.g. Sony, Time-Warner, etc. decides to allow the **Electronic Digital Content Store(s)** 103 to sell its Content 113, the ClearingHouse(s) 105 is contacted, usually via E-mail, with a request that the **Electronic Digital** Content Store(s) 103 be added to the Secure **Digital** Content **Electronic** Distribution System 100. The **digital** content label provides the name of the **Electronic Digital** Content Store(s) 103 and any other information that may be required for the ClearingHouse(s) 105 to create a **digital** certificate for the **Electronic Digital** Content Store(s) 103. The **digital** certificate is sent to the **digital** content label in a secure fashion, and then forwarded by the **digital** content label to the **Electronic Digital** Content Store(s) 103. The ClearingHouse(s) 105 maintains a database of **digital** certificates that it has assigned. Each certificate includes a version number, a unique serial number, the signing algorithm, the name of the issuer (e.g., the name of ClearingHouse(s) 105), a range of dates for which the certificate is considered to be valid, the name **Electronic Digital** Content Store(s) 103, the public key of the **Electronic Digital** Content Store(s) 103, and a hash code of all of the other information signed using the private key of the ClearingHouse(s) 105. Entities... ...that a SC(s) with a signature that can be validated using the public key from the certificate is a valid SC(s).

After the **Electronic Digital** Content Store(s) 103 has received its **digital** certificate that was created by the ClearingHouse(s) 105 and the necessary tools for processing the SC(s) from the **digital** content label, it can begin offering Content 113 that can be purchased by End-User(s). The **Electronic Digital** Content Store(s) 103 includes its certificate and the Transaction SC(s) 640 and signs the SC(s) using its **Digital** Signature 643. The End-User Device(s) 109 verifies that the **Electronic Digital** Content Store(s) 103 is a valid distributor of Content 113 on the Secure **Digital** Content **Electronic** Distribution System 100 by first checking the **digital** certificate revocation list and then using the Public Key 621 of the ClearingHouse(s) 105 to verify the information in the **digital** certificate for the **Electronic Digital** Content Store(s) 103. A **digital** certificate revocation list is maintained by the ClearingHouse(s) 105. The revocation list may be included as one of the parts in a **License** SC(s) 660 that is created by the ClearingHouse(s) 105. End-User Device(s) 109 keep a copy of the revocation list on the End-User Device(s) 109 so they can use it as part of the **Electronic Digital** Content Store(s) 103 **digital** certificate validation. Whenever the End-User Device(s) 109 receives a **License** SC(s) 660 it determines whether a new revocation list is included and if so, the local revocation list on the End-User Device(s) 109 is updated.

B. **Rights** Management Processing

Order SC(s) Analysis

The ClearingHouse(s) 105 receives an Order SC(s) 650 from an End-User(s) after the End-User(s) has received the Transaction SC(s) 640, which include the Offer SC(s) 641, from the **Electronic Digital** Content Store(s) 103. The Order SC(s) 650 consists of parts that contain information relative to the Content 113 and its use, information about the **Electronic Digital** Content Store(s) 103 that is selling the Content 113, and information about the End-User(s) that is purchasing the Content 113. Before the...it contains has not been corrupted in any way.

Validation

The ClearingHouse(s) 105 begins the validation of Order SC(s) 650 by verifying the **digital** signatures, then the ClearingHouse(s) 105 verifies the integrity of the Order SC(s) 650 parts. To validate the **digital** signatures, first the ClearingHouse(s) 105 decrypts the Contents 631 of the signature itself using the Public Key 661 of the signing entity included if signed. (The signing entity could be the Content Provider(s) 101, the **Electronic Digital** Content Store(s) 103, the End User Device(s) 109 or any combination of them.) Then, the ClearingHouse(s) 105 calculates the digest of the concatenated part digests of the SC(s) and compares it with the **digital** signature's decrypted Content 113. If the two values match, the **digital** signature is valid. To verify the integrity of each part, the ClearingHouse(s) 105 computes the digest of the part and compares it to the digest value in the BOM. The ClearingHouse(s) 105 follows the same process to verify the **digital** signatures and part integrity for the Metadata and Offer SC(s) 641 parts included within the Order SC(s) 650.

The process of verification of the Transaction and Offer SC(s) 641 **digital** signatures also indirectly verifies that the **Electronic Digital** Content Store(s) 103 is authorised by the Secure **Digital** Content **Electronic** Distribution System 100. This is based on the fact that the ClearingHouse(s) 105 is the issuer of the certificates. Alternately, the ClearingHouse(s) 105 would be able to successfully verify the **digital** signatures of the Transaction SC(s) 640 and Offer SC(s) 641 using the public key from the **Electronic Digital** Content Store(s) 103, but only if the entity signing the SC(s) has ownership of the associated private key. Only the **Electronic Digital** Content Store(s) 103 has ownership of the private key. Notice that the ClearingHouse(s) 105 does not need to have a local database of the **Electronic Digital** Content Store(s) 103. Since the store uses the Clearinghouse Public Key to sign the Transaction SC(s) 640 Offer SC(s) 641 public keys... ...watermarking instructions are done by the ClearingHouse(s) 105 after authenticity and the integrity check of the Order SC(s) 650, the validation of the **Electronic Digital** Content Store(s) 103, and the validation of the Store Usage Conditions 519 have been completed successfully. The Metadata SC(s) 620 portion of the... ...s) 109 is retrieved from the Order SC(s) 650. The new

encrypted Symmetric Keys 623 are included in the Key Description part of the **License** SC(s) 660 that the ClearingHouse(s) 105 returns to the End-User Device(s) 109.

During the time of processing the Symmetric Keys 623... ...the Symmetric Keys 623, the watermarking instructions are modified and re-encrypted. The new watermarking instructions are included as one of the parts within the **License** SC(s) 660 that gets returned to the End-User Device(s) 109.

If all of the processing of the Order SC(s) 650 is successful, then the ClearingHouse(s) 105 returns a **License** SC(s) 660 to the End-User Device(s) 109. The End-User Device(s) 109 uses the **License** SC(s) 660 information to download the Content SC(s) 630 and access the encrypted Content 113 and metadata. The watermarking instructions are also executed... ...to successfully process the Order SC(s) 650, then an HTML page is returned to the End-User Device(s) 109 and displayed in an **Internet** browser window. The HTML page indicates the reason that the ClearingHouse(s) 105 was unable to process the transaction.

In an alternate embodiment, if the user has purchased a copy of the Content 113 prior to the release date set for the sale, the **License**(s) SC 660 is returned without the Symmetric Keys 623. The **License**(s) SC 660 ...the End-User(s) resides, then the ClearingHouse(s) 105 insures that the transaction being processed is not violating any of those restrictions before transmitting **License** SC(s) 660 to the End-User Device(s) 109. The **Electronic Digital** Content Store(s) 103 is also expected to participate in managing the distribution of Content 113 to various countries by performing the same checks as the ClearingHouse(s) 105. The ClearingHouse(s) 105 does whatever checking that it can in case the **Electronic Digital** Content Store(s) 103 is ignoring the country specific rules set by the Content Provider(s) 101.

D. Audit Logs and Tracking

The ClearingHouse(s... ...during Content 113 purchase transactions and report request transactions. The information can be used for a variety of purposes such as audits of the Secure **Digital** Content **Electronic** Distribution System 100, generation of reports, and data mining.

The ClearingHouse(s) 105 also maintains account balances in Billing Subsystem 182 for the **Electronic Digital** Content Store(s) 103. Pricing structures for the **Electronic Digital** Content Store(s) 103 is provided to the ClearingHouse(s) 105 by the **digital** content labels. This information can include things like current specials, volume discounts, and account deficit limits that need to be imposed on the **Electronic Digital** Content Store(s) 103. The ClearingHouse(s) 105 uses the pricing information to track the balances of the **Electronic Digital** Content

Store(s) 103 and insure that they do not exceed their deficit limits set by the Content Provider(s) 101.

The following operations are typically logged by the ClearingHouse(s) 105:

* End-User Device(s) 109 requests for **License** SC(s) 660

* Credit card authorisation number when the ClearingHouse(s) 105 handles the billing

* Dispersement of **License** SC(s) 660 to End-User Device(s) 109

* Requests for reports

* Notification from the End-User(s) that the Content SC(s) 630 and **License** SC(s) 660 were received and validated

The following information is typically logged by the ClearingHouse(s) 105 for a **License** SC(s) 660:

* Date and time of the request

* Date and time of the purchase transaction

* Content ID of the item being purchased

* Identification of the Content Provider(s) 101

* Store Usage Conditions 519

* Watermarking instruction modifications

* Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103

* Identification of the **Electronic Digital** Content Store(s) 103

* Identification of the End-User Device(s) 109

* End-User(s) credit card information (if the ClearingHouse(s) 105 is handling... ...time of the request

* Amount charged to the credit card

* Content ID of the item being purchased

* Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103

* Identification of the **Electronic Digital** Content Store(s) 103

* Identification of the End-User(s)

* End-User(s) credit card information

* Authorisation number received from the clearer of the credit card

The following information is typically logged by the ClearingHouse(s) 105 when a **License** SC(s) 660 is sent to an End-User Device(s) 109:

* Date and time of the request

* Content ID of the item being purchased

* Identification of Content Provider(s) 101

* Usage Conditions 517

* Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103

* Identification of the **Electronic Digital** Content Store(s) 103

* Identification of the End-User(s)

The following information is typically logged when a report request is made:

* Date and time... ...by the ClearingHouse(s) 105 using the information that the ClearingHouse(s) 105 logged during End-User(s) purchase transactions. Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103 can request transaction reports from the ClearingHouse(s) 105 via a Payment Verification Interface 183 so they can reconcile their own... ...with the information logged by the ClearingHouse(s) 105. The ClearingHouse(s) 105 can also provide periodic reports to the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103.

The ClearingHouse(s) 105 defines a secure **electronic** interface which allows Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103 to request and receive reports. The Report Request SC(s) includes a certificate that was assigned by the ClearingHouse(s) 105 to the entity initiating the request. The ClearingHouse(s) 105 uses the certificate and the SC's **digital** signature to verify that the request originated from an authorised entity. The request also includes

parameters, such as time duration, that define the scope of...version of this document.

F. Billing and Payment Verification

Billing of Content 113 can be handled either by the ClearingHouse(s) 105 or by the **Electronic Digital** Content Store(s) 103. In the case where the ClearingHouse(s) 105 handles the billing of the **electronic** Content 113, the **Electronic Digital** Content Store(s) 103 separates the End-User(s)' order into **electronic** goods and, if applicable, physical goods. The **Electronic Digital** Content Store(s) 103 then, notifies the ClearingHouse(s) 105 of the transaction, including the End-User(s)' billing information, and the total amount that needs to be authorised. The ClearingHouse(s) 105 authorises the End-User(s)' credit card and returns a notification back to the **Electronic Digital** Content Store(s) 103. At the same time the ClearingHouse(s) 105 is authorising the End-User(s)' credit card, the **Electronic Digital** Content Store(s) 103 can charge the End-User(s)' credit card for any physical goods that are being purchased. After each **electronic** item is downloaded by the End-User Device(s) 109, the ClearingHouse(s) 105 is notified so the End-User(s)' credit card can be... ...End-User Device(s) 109 before the Content 113 is enabled for use at the End-User Device(s) 109.

In the case where the **Electronic Digital** Content Store(s) 103 handles the billing of the **electronic** Content 113, the ClearingHouse(s) 105 is not notified about the transaction until the End-User Device(s) 109 sends the Order SC(s) 650 to the ClearingHouse(s) 105. The ClearingHouse(s) 105 is still notified by the End-User Device(s) 109 after each **electronic** item is downloaded. When the ClearingHouse(s) 105 is notified it sends a notification to the **Electronic Digital** Content Store(s) 103 so that the **Electronic Digital** Content Store(s) 103 can charge the End-User(s)' credit card.

G. Retransmissions

The Secure **Digital** Content **Electronic** Distribution System 100 provides the ability to handle retransmissions of Content 113. This is typically performed by a Customer Service Interface 184. **Electronic Digital** Content Store(s) 103 provides a user interface that the End-User(s) can step through in order to initiate a retransmission. The End-User(s) goes to the **Electronic Digital** Content Store(s) 103 site where the Content 113 item was purchased in order to request a retransmission of the Content 113.

Retransmissions of Content... ...a previously purchased Content 113 item because the Content 113 could not be downloaded or the Content 113 that was

downloaded is not usable. The **Electronic Digital** Content Store(s) 103 determines whether the End-User(s) is entitled to do a retransmission of the Content 113. If the End-Users) is entitled to a retransmission, then the **Electronic Digital** Content Store(s) 103 builds a Transaction SC(s) 640 that includes the Offer SC(s) 641 of the Content 113 item(s) being retransmitted... ...s) 109 to delete the scrambled key(s).

In the case where the ClearingHouse(s) 105 handles the financial settlement of Content 113 purchases, the **Electronic Digital** Content Store(s) 103 includes a flag in the Transaction SC(s) 640 that is carried forward to the ClearingHouse(s) 105 in the Order... ...charging the End-User(s) for the purchase of the Content 113.

VIII. CONTENT PROVIDER

A. Overview

The Content Provider(s) 101 in the Secure **Digital** Content **Electronic** Distribution System 100 is the **digital** content label or the entity who owns the **rights** to the Content 113. The role of the Content Provider(s) 101 is to prepare the Content 113 for distribution and make information about the Content 113 available to **Electronic Digital** Content Store(s) 103 or retailers of the downloadable **electronic** versions of the Content 113. To provide the utmost security and **rights** control to the Content Provider(s) 101, a series of tools are provided to enable the Content Provider(s) 101 to prepare and securely package... ...domain and never exposed or accessible by unauthorised parties. This allows Content 113 to be freely distributed throughout a non-secure network, such as the **Internet**, without fear of exposure to hackers or unauthorised parties.

The end goal of the tools for the Content Provider(s) 101 is to prepare and an **audio** example any required equalisation, dynamics adjustment, or re-sampling) encoding and compression.

* Metadata Assimilation and Entry Tool 161 - A collection of tools **used** to gather **Content** 113 description information from the Database 160 of the Content Provider(s) and/or third party database or data import files and/or via operator interaction and provides means for specifying content Usage Conditions 517. Also provided is an interface for capturing or extracting content such as **digital audio** content for CDS or DDP files.

* Quality Control Tool enables to preview of prepared content and metadata. Any corrections needed to the metadata or resubmission... ...to pack into SC(s).

* Content Dispersement Tool (not shown) - Disperses SC(s) to designated distribution centres, such as Content Hosting Site(s) 111 and **Electronic Digital Content Store(s)** 103.

* Content Promotions **Web** Site 156 - stores Metadata SC(s) 620 and optionally additional promotional material for download by authorised **Electronic Digital Content Store(s)** 103.

B. Work Flow Manager 154

The purpose of this tool is to schedule, track, and manage Content 113 processing activities. This... ...or as any of it's constitute processes may be distributed as an application program in a computer readable medium including but not limited to **electronic** distribution such as the **web** or on floppy diskettes, CD ROMS and removable hard disk drives.

Turning now to FIG. 8 is a block diagram of the major processes of...information is entered to uniquely identify the product. Optionally, additional fields may be included to request manual entry of the information required to initiate the **audio** processing phase in parallel with the metadata acquisition. If not provided manually, this information can optionally be retrieved from default configuration settings or from the... ...to the Database 160 of the Content Provider(s) 101 is specified, the job is processed by the Automatic Metadata Acquisition Process 803. In a **music** embodiment, to properly schedule the product for **audio** processing, the product's genre and the desired compression levels are specified as well as the **audio** PCM or WAV filename(s). This information may be entered as part of the product selection process or selected via a customised query interface or **Web** browser function. Specification of this information enables the product to be scheduled for content processing.

The product selection user interface provides an option enabling the... ...Manual Metadata Entry Process 804 (see Automatic Metadata Acquisition Process 803 section for details on the Database Mapping Table).

If the required general information for **audio** processing and the specific information required for watermarking is specified, the job is queued for Watermarking Process 808 (the first phase of content processing). If... ...status indicating the information that is missing.

If the status indicates that the filename of the Content 113, for example where the Content 113 is **audio** and the PCM or WAV file is missing, this may indicate that a capture (or **digital** extraction from **digital** media) is required. The **audio** processing functions require that the song files be accessible via a standard file system interface. If the songs are located on external media or a file system that is

not directly accessible to the **audio** processing tools, the files are first be copied to an accessible file system. If the songs are in **digital** format but on CD or **Digital** Tape, they are extracted to a file system accessible to the **audio** processing tools. Once the files are accessible, the Work Flow Manager User Interface 700 is used to specify or select the path and filename for... ...160 of the Content Provider(s) 101 to obtain the information necessary to process this Content 11)3. For example, if the Content 113 is **music**, the information needed to perform this query could be the album name or may be a UPC or a specific album or selection ID as...Action/Information Process 801.

6. Supervised Release Process 806

The Supervised Release Process 806 allows a quality check and validation of information specified for the **digital** content product. It does not have any dependencies. Comments previously attached to the job at any stage of the processing for this product can be... ...the usage conditions

* the encryption keys used in the encryption stage of all quality levels for this product

This last dependency requires that the associated **audio** objects completed the **audio** processing phase before the Metadata SC(s) 620 can be created. Upon completion of the Metadata SC(s) Creation Process 807, the job is queued... ...Encryption Process 811.

If third party providers of encoding tools do not provide a method to display the percentage of the Content 113, such as **audio**, that has been processed or a method to indicate the amount of Content 113 that has been encoded as a percentage of the entire selection of Content 113 selected, in FIG. 11 there is shown a flow diagram 1100 of a method to determine the encoding rate of **Digital** Content for the Content Preprocessing and Compression tool of FIG. 8. The method begins with the selection of the desired encoding algorithm and a bit... ...rate factor RNEW. Calculating a new rate factor RNEW knowing the amount of time and the amount of Content 113 encoded is RNEW = (length of **Digital** Content encoded)/(amount of time), step 1108. The Content 113 is encoded and the encoding status is displayed using the previously calculate rate factor RNEW...of the song file remain available until after Content Quality Control Process 810.

11. Encryption Process 811

The Encryption Process 811 calls the appropriate Secure **Digital** Content **Electronic** Distribution **Rights** Management function to encrypt each of the watermarked/encoded song files. This process has no dependencies other than completion of all other **audio** processing. Upon completion of the Encryption Process 811 process, the job is queued for Content SC(s) Creation Process 812.

12. Content SC(s) Creation...product/quality level) tuple triggers an action).

C. Metadata Assimilation and Entry Tool

Metadata consists of the data describing the Content 113 for example in **music**, title of the recording, artist, author/composer, producer and length of recording. The following description is based upon Content 113 being **music** but it should be understood by those skilled in the art that other content types e.g., video, programs, multimedia, **movies**, and equivalent, are within the true scope and meaning of the present invention.

This Subsystem brings together the data the Content Provider(s) 101 provides to the **Electronic Digital** Content Store(s) 103 to help promote the sale of the product (e.g., for **music**, sample clips by this artist, history of this artist, list of albums on which this recording appears, genres associated with this artist and/or product... ...Provider(s) 101 wants to offer the End-User(s). The data is packaged into a Metadata SC(s) 620 and made available to the **Electronic Digital** Content Store(s) 103. To accomplish this, the following tools are provided:

* Automatic Metadata Acquisition Tool

* Manual Metadata Entry Tool

* Usage Conditions Tool

* Supervised Release... ...to End-User(s) (e.g., composer, producer, sidemen, track length) and the types of promotional data the Content Provider(s) 101 provides to the **Electronic Digital** Content Store(s) 103 (e.g., for a **music** example, sample clips by this artist, a history of this artist, the list of albums on which this recording appears, genres associated with this artist... ...109, data fields which can be optionally provided to the End-User Device(s) 109 and a sample set of data fields, targeted to the **Electronic Digital** Content Store(s) 103, that promote the artist, album, and/or single.

To extract the template data fields from the Database 160 of the Content... ...user the ability to implement the Usage Conditions Process 805 described above. The

process of offering Content 113 for sale or rent (Limited use), using **electronic** delivery, involves a series of business decisions. The Content Provider(s) 101 decides at which compression level(s) the Content 113 is made available. Then for each compressed encoded version of the Content 113, one or more usage conditions are specified. Each usage condition defines the **rights** of the End-User(s), and any restrictions on the End-User(s), with regard to the use of the Content 113.

As part of Content Processing Tools 155, a set of usage conditions (End-User(s) **rights** and restrictions) is attached to the product.

A usage condition defines:

1. the compression encoded version of the Content 113 to which this usage condition... ...condition allows for the purchase or the rental of the Content 113. For a rental transaction:

the measurement unit which is used to limit the **term** of the rental (e.g., days, plays).

the number of the above units after which the Content 113 will no longer play.

For a purchase... ...the period of time during which the purchase/rental transaction is allowed to occur (i.e., an End-User(s) can purchase/rent under the **terms** of this usage condition only after the beginning availability date and before the last date of availability).

5. the countries from which an End-User...the retail channel.

D. Content Processing Tools

The Content Processing Tools 155 is actually a collection of software tools which are used to process the **digital** content file to create watermarked, encoded, and encrypted copies of the content. The tools makes use of industry standard **digital** content processing tools to allow pluggable replacement of watermarking, encoding and encryption technologies as they evolve. If the selected industry tool can be loaded via... ...C/C++ or any equivalent software. The Content Processing Tools 155 can be delivered by any computer readable means including diskettes, CDS or via a **Web** site.

1. Watermarking Tool

The Watermarking Tool provides a user the ability to implement the Watermarking Process 808 as described above. This tool applies copyright information of the Content 113 owner to the song file using **audio** Watermarking technology. The actual information to be written out is determined by the Content Provider(s) 101 and the specific watermarking technology selected. This information... ...requirement on the Metadata Assimilation and Entry Tool 161 to assure that it has acquired this information prior to, for example, allowing the song's **audio** file to be processed. This song will not be available for **audio** processing until the watermarking information has been obtained.

The watermark is applied as the first step in **audio** processing since it is common to all encodings of the song created. As long as the watermark can survive the encoding technology, the watermarking process... ...Preprocessing and Compression Tool

The Preprocessing and Compression Tool provides a user the ability to implement the Preprocessing and Compression Process 809 as described above. **Audio** encoding involves two processes. Encoding is basically the application of a lossy compression algorithm against, for a **music** content example, a PCM **audio** stream. The encoder can usually be tuned to generate various playback bit stream rates based on the level of **audio** quality required. Higher quality results in larger file sizes and since the file sizes can become quite large for high quality Content 113, download times... ...can become lengthy and sometimes prohibitive on standard 28,800 bps modems.

The Content Provider(s) 101 may, therefore, choose to offer a variety of **digital** content qualities for download to appease both the impatient and low bandwidth customers who don t want to wait hours for a download and the... ...to the compression algorithm. To allow for more efficient compression with less loss of fidelity or to prevent drastic dropout of some frequency ranges, the **digital** content may sometimes require adjustments to equalisation levels of certain frequencies or adjustments to the dynamics of the recording. The content preprocessing requirements are directly related to the compression algorithm and the level of compression required. In some cases, the style of Content 113 (e.g. **musical** genre) can be successfully used as a base for determining preprocessing requirements since songs from the same genre typically have similar dynamics. With some compression tools, these preprocessing functions are part of the encoding process. With others, the desired preprocessing is performed prior to the compression.

Besides the downloadable **audio** file for sale, each song also has a Low Bit Rate (LBR) encoded clip to allow the song to be sampled via a LBR streaming...

...compression. The front end Encoding Tool may have a synchronisation requirement with the Metadata Assimilation and Entry Tool 161, for example if the content is **music**, and if it is determined that the song's genre is acquired from the Database 160 of the Content Provider(s) prior to performing any **audio** preprocessing. This depends on the encoding tools selected and how indeterminate the genre for the song is. If the Content Provider(s) 101 varies the...

...present invention. The process starts with reading an identifier from the media the Content Provider(s) 101 is examining. One example of content in an **audio** CD embodiment. In an **audio** CD embodiment, the following codes may be available Universal Price Code (UPC), International Standard Recording Code (ISRC), International Standard **Music** Number (ISMN). This identifier is read in the appropriate player for the content, for example an **audio** CD Player for **audio** CD, DVD player for DVD **movie**, DAT recorder for DAT recording and equivalent, step 1201. Next this Identifier is used to index a Database 160 for the Content Provider(s) 101... ...113 and the metadata related to it. In step 1204, the additional information retrieved is used to start the Work Flow Manager 154 for creating **electronic** Content 113. It should be understood, that several selections of media, such as several **audio** CDS, can be queued up so as to enable the Automatic Metadata Acquisition Tool to create a series of Content 113 for **electronic** distribution. For example, all the Content 113 could be created from a series of CDS or even selected tracks from one or more CDS examined...

...Preprocessing and Compression parameters of the Preprocessing and Compression Tool of FIG. 8 according to the present invention. In this embodiment. the Content 113 is **music**. In step 1301, **music** (Content 113) is selected to be encoded in Content Processing Tools 155. The genre of the **music** selected is determined, step 1302. This can be entered manually or by using other meta data available, such as the additional data retrieved from the process described in FIG. 12. The **audio** compression level and **audio** compression algorithms selected are than examined, step 1303. Next, a lookup is made by genre, compression settings and compression algorithms of what compression parameters should...630. This process creates a single Metadata SC(s) 620 and multiple Content SC(s) 630 for each song. For example, if the content is **music**, each of the **audio** files created during **audio** processing for the various quality levels of the full song is packed into separate Content SC(s) 630. The **audio** file created for the sample clip is passed as a metadata file to be included in the Metadata SC(s) 620.

F. Final Quality Assurance... ...101 can choose to perform quality assurance as each major step is completed to prevent excessive rework later or may choose to wait until all **audio** preparation processes are complete and perform quality assurance on everything at once. If the latter is chosen, quality assurance is performed at this point upon completion of the creation of the SC(s). This tool allows each SC(s) for the song to be opened, examined, and the **audio** played.

Any problem discovered, even minor text changes requires that the SC(s) be rebuilt due to internal security features of SC(s). To avoid... ...101 to prepare content in advance of their scheduled release date and hold them until they wish to release them e.g., a new song, **movie** or game. The SC(s) can also control access to Content 113 based on a defined release date so there is no requirement for the... ...are transferred via FTP to the designated Content Hosting Site(s) 111. The Metadata SC(s) 620 is transferred via FTP to the Content Promotions **Web** Site 156. Here the SC(s) are staged to a new Content 113 directory until they can be processed and integrated into the Content Promotions **Web** Site 156.

FIG. 17 is a flow diagram of an alternate embodiment to automatically retrieve additional information for the Automatic Metadata Acquisition Tool of FIG...Manual Metadata Entry 803. Since, many of the usage conditions can be automatically filled-in during the Automatic Metadata Acquisition 803 step.

H. Content Promotions **Web** Site

To most effectively disperse information on what the Content Provider(s) 101 is making available for sale via **digital** download, and to get the necessary files to the **Electronic Digital** Content Store(s) 103 to enable it to make this Content 113 available for download to its customers, each Content Provider(s) 101 should have a secure **web** site housing this information. This is similar to the method used today by some Content Provider(s) 101 to make promotional content available to their... ...others with a need for this information. In the case where this type of service already exists, an additional section can be added to the **web** site where **Electronic Digital** Content Store(s) 103 can go to see a list of the content available for sale via download.

The Content Provider(s) 101 has complete control over the design and layout of this site or can choose to use a turnkey **web** server solution provided as part of the toolkit for Secure **Digital** Content **Electronic** Distribution System 100. To implement their own design for this service, the Content Provider(s) 101 need only provide links to the Metadata SC(s) 620 for **Electronic Digital** Content Store(s) 103 who access their site. This is accomplished using the toolkit for the Secure **Digital** Content **Electronic** Distribution System 100. The selection process and what information is shown is the discretion of the Content Provider(s) 101.

Metadata SC(s) 620 received into a new content directory via FTP from the Content Dispersement Tool is processed by the Content Promotions **Web** Site 156. These containers can be opened with the SC(s) Preview Tool to display or extract information from the container. This information can then be used to update HTML **Web** pages and/or add information to a searchable database maintained by this service. The SC(s) Preview Tool is actually a subset of the

Content Acquisition Tool **used** by the **Electronic Digital** Content Store(s) 103 to open and process Metadata SC(s) 620. See the Content Acquisition Tool section for more details. The Metadata SC(s) 620 file should then be moved to a permanent directory maintained by the Content Promotions **Web** Site 156.

Once the Metadata SC(s) 620 has been integrated into the Content Promotions **Web** Site 156, its availability is publicised. The Content Provider(s) 101 can send a notification to all subscribing **Electronic Digital** Content Store(s) 103 as each new Metadata SC(s) 620 is added to the site or can perform a single notification daily (or any defined periodicity) of all Metadata SC(s) 620 added that day (or period). This notification is performed via a standard HTTP exchange with the **Electronic Digital** Content Store(s) 103 **Web** Server by sending a defined CGI string containing parameters referencing the Metadata SC(s) 620 added. This message is handled by the Notification Interface Module of the **Electronic Digital** Content Store(s) 103 which is described later.

I. Content Hosting

The Entertainment Industry produces thousands of content titles, such as CDS, **movies** and games every year, adding to the tens of thousands of content titles that are currently available. The Secure **Digital** Content **Electronic** Distribution System 100 is designed to support all of the content titles available in stores today.

The numbers of content titles that the Secure **Digital** Content **Electronic** Distribution System 100 may eventually download to customers on a daily basis is in the thousands or tens of thousands. For a large number of... ...The system also supports customers all over the world. This requires overseas sites to speed delivery to the global customers.

Content hosting on the Secure **Digital** Content **Electronic** Distribution System 100 is designed to allow the Content Provider(s) 101 to either host their own Content 113 or share a common facility or a set of facilities.

Content hosting on the Secure **Digital** Content **Electronic** Distribution System 100 consists of multiple Content Hosting Site(s) 111 that collectively contain all of the Content 113 offered by the Secure **Digital** Content **Electronic** Distribution System 100 and several Secondary Content Sites (not shown) that contain the current hot hits offered by the Content Provider(s) 101. The number... ...single Content Hosting Site 111 with or without additional Secondary Content Sites. This allows them to build their own scalable distributed system. In another embodiment, **Electronic Digital** Content Store(s) 103 can also act as Content Hosting Site(s) 111 for certain Content 113. This embodiment requires a special

financial agreement between the **Electronic Digital** Content Store(s) 103 and the Content Provider(s) 101.

1. Content Hosting Sites

Content 113 is added to the Content Hosting Site(s) 111...field that indicates the URL locating the Content SC(s) 630 for this Content 113. This URL corresponds to a Content Hosting Site(s) 111. **Electronic Digital** Content Store(s) 103 can override this URL if allowed by the Content Provider(s) 101 in the Offer SC(s) 641. The End-User... ...to download the Content SC(s) 630.

The End-User Device(s) 109 initiates the request for a Content SC(s) 630 by sending the **License** SC(s) 660 to the Content Hosting Site(s) 111. This is the same **License** SC(s) 660 returned by the ClearingHouse(s) 105. The **Digital** Signature of the **License** SC(s) 660 can be verified to determine if it is a valid **License** SC(s) 660. If it is a valid **License** SC(s) 660 either the download is initiated, or the download request may be redirected to another Content Hosting Site(s) 111.

2. Content Hosting Site(s) 111 provided by the Secure **Digital** Content **Electronic** Distribution System 100

For the Secure **Digital** Content **Electronic** Distribution System 100 the decision of which site should be used to download the Content 113 is made by the primary content site that received... ...information to make this decision:

* Are there secondary content sites that host the Content 113 requested? (The majority of Content 113 offered by the Secure **Digital** Content **Electronic** Distribution System 100 is only located at primary sites);

* Where is the End-User Device(s) 109 geographically located? (This information can be obtained from... ...the End-User Device(s) 109, analysis and verifications are performed on the End-User's request. A database is kept of all of the **License** SC IDs that have been **used** to download **Content** 113. This database can be checked to ensure that the End-User Device(s) 109 only makes one request for each piece of Content 113... ...the amount of activity on the sites and whether a site is down for maintenance.

The only interface to the Content Hosting Router is the **License** SC(s) 660 that is sent by the End-User Device(s) 109 when Content 113 is required to be downloaded. The **License** SC(s) 660 includes information that indicates the user is allowed to download the Content 113.

Secondary Content Sites

The Secondary Content Sites (not shown) host the popular Content 113 of the Secure **Digital** Content Distribution System 100. These sites are geographically dispersed across the world and are located near Network Access Points (NAPs) to improve download times. These sites are added to the system as demand on the primary Content Hosting Site(s) 111 nears maximum capacity

IX. ELECTRONIC DIGITAL CONTENT STORE(S)

A. Overview - Support for Multiple **Electronic Digital** Content Store(s) 103

Electronic Digital Content Store(s) 103 are essentially the retailers. They are the entities who market the Content 113 to be distributed to the customer. For distribution of Content 113, this would include **Digital** Content Retailing **Web** Sites, **Digital** Content Retail Stores, or any business who wishes to get involved in marketing **electronic** Content 113 to consumers. These businesses can market the sale of **electronic** Content 113 only or can choose to just add the sale of **electronic** goods to whatever other merchandise they currently offer for sale. Introduction of downloadable **electronic** goods into the service offering of the **Electronic Digital** Content Store(s) 103 is accomplished via a set of tools developed for the **Electronic Digital** Content Store(s) 103 as part of the Secure **Digital** Content **Electronic** Distribution System 100.

These tools are used by the **Electronic Digital** Content Store(s) 103 to:

* acquire the Metadata SC(s) 620 packaged by the Content Provider(s) 101

* extract Content 113 from these SC(s... ...the status of each download

* handle status notifications and transaction authentication requests

* perform account reconciliation

The tools are designed to allow flexibility in how the **Electronic Digital** Content Store(s) 103 wishes to integrate sale of downloadable **electronic** Content 113 ...that all financial settlements for downloadable Content 113 purchased be handled by the ClearingHouse(s) 105 although this is not required. These tools also enable **Electronic Digital** Content Store(s) 103 to completely service their customers and handle the financial transactions themselves, including providing

promotions and special offers. The tools enable the **Electronic Digital** Content Store(s) 103 to quickly integrate the sale of downloadable Content 113 into its existing services. In addition, the **Electronic Digital** Content Store(s) 103 is not required to host the downloadable Content 113 and does not have to manage its dispersement. This function is performed by the Content Hosting Site(s) 111 selected by the Content Provider(s) 101.

The tools for the **Electronic Digital** Content Stores(s) 103 are implemented in Java in the preferred embodiment but other programming languages such as C/C++, Assembler and equivalent can be used. It should be understood that the tools described below for the **Electronic Digital** Content Stores(s) 103 can run on a variety of hardware and software platforms. The **Electronic Digital** Content Stores(s) 103 as a complete system or as any of it's constitute components may be distributed as an application program in a computer readable medium including but not limited to **electronic** distribution such as the **web** or on floppy diskettes, CD ROMS and removable hard disk drives.

In another embodiment, the components of the **Electronic Digital** Content Stores(s) 103 is part of a programmer's software toolkit. This toolkit enables predefined interfaces to the components of the generic **Electronic Digital** Content Stores(s) 103 components and tools discussed below. These predefined interfaces are in the form of APIs or Application Programming Interfaces. A developer using... ...of the functionality of the components from a high level application program. By providing APIs to these components, a programmer can quickly develop a customised **Electronic Digital** Content Stores(s) 103 without the need to re-created these functions and resources of any of these components.

Electronic Digital Content Store(s) 103 are not limited to **Web** based service offerings. The tools provided are used by all **Electronic Digital** Content Store(s) 103 wishing to sell downloadable **electronic** Content 113 regardless of the transmission infrastructure or delivery mode used to deliver this Content 113 to End-User(s). Broadcast services offered over satellite and cable infrastructures also use these same tools to acquire, package, and track **electronic** Content 113 sales. The presentation of **electronic** merchandise for sale and the method in which these offers are delivered to the End-User(s) is the main variant between the broadcast based service offering and the point-to-point interactive **web** service type offering.

B. Point-to-Point **Electronic Digital** Content Distribution Service

Point-to-Point primarily means a one-to-one interactive service between the **Electronic Digital** Content Store(s) 103 and the End-User Device(s) 109. This typically represents an **Internet web** based service provided via telephone or cable modem connection. Networks other than the **Internet** are supported in this

model as well, as long as they conform to the **Web** Server/Client Browser model. FIG. 9 is a block diagram illustrating the major tools, components and processes of an **Electronic Digital** Content Store(s) 103.

1. Integration Requirements

The Secure **Digital** Content **Electronic** Distribution System 100 not only creates new **online** businesses but provides a method for existing businesses to integrate the sale of downloadable **electronic** Content 113 to their current inventory. The suite of tools provided to the **Electronic Digital** Content Store(s) 103 simplify this integration effort. The Content Acquisition Tool 171 and SC(s) Packer Tool 153 provides a method for the **Electronic Digital** Content Store(s) 103 to acquire information from the participating Content Provider(s) 101 on what they have available for sale and to create the... ...is batch driven and can be largely automated and is executed only to integrate new Content 113 into the site.

The tools for the Secure **Digital** Content **Electronic** Distribution have been designed to allow integration of sale of **electronic** downloadable Content 113 into typical implementations of **web** based **Electronic Digital** Content Store(s) 103 (i.e. Columbia House **online**, **Music** Boulevard, @Tower) and equivalent with minimal change to their current Content 113 retailing paradigm. Several methods of integration are possible and in the preferred embodiment, the **Electronic Digital** Content Store(s) 103 provides support for all product searches, previews, selections (shopping cart), and purchases. Each **Electronic Digital** Content Store(s) 103 establishes customer loyalty with its customers and continues to offer its own incentives and market its products as it does today. In the Secure **Digital** Content **Electronic** Distribution System 100, it would simply need to indicate which products in its inventory are also available for **electronic** download and allow its customers to select the **electronic** download option when making a purchase selection. In another embodiment, the customer's shopping cart could contain a mixture of **electronic** (Content 113) and physical media selections. After the customer checks out, and the **Electronic Digital** Content Store(s) 103 has completed the financial settlement and logged or notified its shipping and handling functions to process the physical merchandise purchased, the commerce handling function of the **Electronic Digital** Content Store(s) 103 then calls the Transaction Processor Module 175 to handle all **electronic** downloads. It simply passes the required information and all processing from that point on is handled by the toolset for the Secure **Digital** Content **Electronic** Distribution System 100. In another embodiment, other methods of transaction handling are also possible using tools for the Secure **Digital** Content **Electronic** Distribution System 100 to handle the financial settlement should the **Electronic Digital** Content Store(s) 103 wish to sell downloadable merchandise only or to segregate the financial settlement of physical and downloadable merchandise.

To handle the downloading of merchandise, the **Electronic Digital** Content Store(s) 103 is given a Product ID (not shown) for each downloadable product that it acquires from the Content Promotions **Web** Site 156 for the Content Provider(s) 101. This Product ID is associated to a customer's purchase selection to the downloadable product. The Product ID is what the **Electronic Digital** Content Store(s) 103 passes to the Transaction Processor Module 175 to identify the product that the user has purchased. The SC(s) (Offer SC(s) 641) that were created to describe the products, are isolated from the **Electronic Digital** Content Store(s) 103 and kept in an Offer Database 181 in an effort to simplify management of these objects and make their existence transparent to the **Electronic Digital** Content Store(s) 103.

The Transaction Processor Module 175 and other additional functions are provided as **web** server side executables (i.e. CGI and NSAPI, ISAPI callable functions) or simply APIs into a DLL or C object library. These functions handle run time processing for End-User(s) interactions and optional interactions with the ClearingHouse(s) 105. These functions interact with the **web** server's commerce services to create and download to the End-User Device(s) 109 the files necessary to initiate the Content 113 download process... ...also handle optional interactions to provide authorisations and accept notifications of completion of activities.

An Accounting Reconciliation Tool 179 is also provided to assist the **Electronic Digital** Content Store(s) 103 in contacting the ClearingHouse(s) 105 to reconcile accounts based on its own and the transaction logs of the ClearingHouse(s) 105.

2. Content Acquisition Tool 171

The Content Acquisition Tool 171 is responsible for interfacing with the Content Promotions **Web** Site 156 to preview and download Metadata SC(s) 620. Since the Content Promotions site is a standard **web** site, a **web** browser is used by the **Electronic Digital** Content Store(s) 103 to navigate this site. The navigation features varies based on the site design of the Content Provider(s) 101. Some sites... ...from. All sites include the selection of Metadata SC(s) 620 containing all the promotional and descriptive information of a song or album.

Alternatively, the **Electronic** Store(s) 103 may subscribe to content updates and receive updates automatically via FTP.

Viewing Metadata

The Content Acquisition Tool 171 is a **web** browser helper application which launches whenever a Metadata SC(s) 620 link is selected at the Content

Promotions **Web** Site 156. Selection of the SC(s) causes it to be downloaded to the **Electronic Digital** Content Store(s) 103, and launch the helper application. The Content Acquisition Tool 171 opens the Metadata SC(s) 620 and display the non-encrypted information contained therein. Displayed information includes Extracted Metadata 173, for a **music** example, the graphic image(s) associated with the song and the information describing the song, a preview clip of the song can also be listened to if included in the Metadata SC(s) 620. In an example where the Content 113 is **music**, promotional information about the song or album, the album title, and the artist is also shown if provided by the Content Provider(s) 101. This... ...as the song and the lyrics and whatever other metadata the Content Provider(s) 101 wishes to protect, is not accessible to the Retail Content **Web** Site 180.

In another embodiment, the Content Provider(s) 101 provides optional promotional content for a fee. In this embodiment such promotional content is encrypted in the Metadata SC(s) 620. Financial settlement to open this data can be handled via the ClearingHouse(s) 105 with the account for the **Electronic Digital** Content Store(s) 103 being charged the designated fee.

Extracting Metadata

Besides the preview capabilities, this tool provides two additional features: metadata extraction and preparation of an Offer SC(s) 641. Selection of the metadata extraction option prompts the **Electronic Digital** Content Store(s) 103 to enter the path and filenames to where the metadata is to be stored. Binary metadata such as graphics and the **audio** preview clip is stored as separate files. Text metadata is stored in an ASCII delimited text file which the Retail Content **Web** Site 180 can then import into its database. A table describing the layout of the ASCII delimited file is also be created in a separate... ...One important piece of information provided in the extracted data is the Product ID. This Product ID is what the commerce handling function for the **Electronic Digital** Content Store(s) 103 needs to identify to the Transaction Processor Module 175 (for more information refer to Transaction Processing section), the Content 113 that... ...to properly retrieve the appropriate Offer SC(s) 641 from the Offer Database 181 for subsequent download to the End-User Device(s) 109. The **Electronic Digital** Content Store(s) 103 has full control over how it presents the offer of downloadable Content 113 on its site. It only needs to retain a cross reference of the Content 113 being offered to this Product ID to properly interface with the tools for the Secure **Digital** Content **Electronic** Distribution System 100. Providing this information here, allows the **Electronic Digital** Content Store(s) 103 to integrate this product or Content 113 into its inventory and sales pages (database) in parallel with the Offer SC(s **Electronic Digital** Content Store(s) 103 is required to create an Offer SC(s) 641 describing the downloadable Content 113 that is for sale. Most of the... ...Template in the Metadata SC(s) 620

* adding additional required parts as defined by defaults specified by the configuration options in this tool for the **Electronic Digital** Content Store(s) 103

* prompting for additional required inputs or selections as defined by the Offer SC(s) Template in the Metadata SC(s) 620... ...later) on the End-User Device(s) 109 is kept in the Metadata SC(s) 620. Other promotional metadata that was only used by the **Electronic Digital** Content Store(s) 103 as input to his **web** service database is removed from the Metadata SC(s) 620. **Rights** management information provided by the Content Provider(s) 101, such as watermarking instructions, encrypted Symmetric Keys 623, and Usage Conditions 517 defining the permitted uses of the object, are also retained.

This stripped down Metadata SC(s) 620 is then included in the Offer SC(s) 641. The **Electronic Digital** Content Store(s) 103 also attaches its own Usage Conditions called Store Usage Conditions 519 or purchase options to the Offer SC(s) 641. This can be accomplished interactively or automatically through a set of defaults. If configured to be processed interactively, the **Electronic Digital** Content Store(s) 103 is prompted with the set of permitted object Usage Conditions 517 as defined by the Content Provider(s) 101. He then... ...option(s) he wishes to offer to his customers. These now become the new Usage Conditions or Store Usage Conditions 519. To process automatically, the **Electronic Digital** Content Store(s) 103 configures a set of default purchase options to be offered for all Content 113. These default options are automatically checked against... ...Database 181 and is indexed with the Product ID pre-assigned in the Metadata SC(s) 620. This Product ID is used later by the **Electronic Digital** Content Store(s) 103 to identify the downloadable Content 113 being purchased by a customer when interfacing with the Offer Database 181 to retrieve the... ...s) 641 for packaging and transmittal to the End-User(s). See the Transaction Processor Module 175 section for more details.

In another embodiment, the **Electronic Digital** Content Store(s) 103 hosts the Content SC(s) 641 at his site. This embodiment requires changes to the Offer SC(s) 641 such as the replacement of the URL of the Content Hosting Site(s) 111 with the URL of the **Electronic Digital** Content Store(s) 103.

3. Transaction Processing Module 175

Electronic Digital Content Store(s) 103 directs billing to ClearingHouse(s) 105. Alternatively, the **Electronic Digital** Content Store(s) 103 may request financial clearance direct from the ClearingHouse(s) 105. There are two basic modes for processing End-User(s) purchase requests for downloadable Content 113. If the **Electronic Digital** Content Store(s) 103 does not wish to handle the financial settlement of the purchase and has no special promotions or incentives governing the sale... ...pricing information included in the metadata. Also included in the

Offer SC(s) 641 is a special HTML offer page presenting the purchase options with **terms** and conditions of the sale. This page is built from a template created when the Offer SC(s) 641 was built. When the End-User... ...this form may contain the fields needed to use the End-User(s)' credit information or industry standard local transaction handler.

An embodiment where the **Electronic Digital** Content Store(s) 103 handles billing is now described. The more typical mode of handling purchase requests is to allow the **Electronic Digital** Content Store(s) 103 to process the financial settlement and then submit the download authorisation to the End-User(s). This method allows the **Electronic Digital** Content Store(s) 103 to integrate sale of downloadable Content 113 with other merchandise offered for sale at his site, allows batch processing of purchase requests with only one consolidated charge to the customer (via a shopping cart metaphor) instead of individual charges for each download request, and allows the **Electronic Digital** Content Store(s) 103 to directly track his customers buying patterns and offer special promotions and club options. In this environment, the offer of downloadable... ...which get added to a shopping cart when selected by the End-User(s) and get processed and financially settled as is done in the **Electronic Digital** Content Store(s)' 103 current shopping model. Once the financial settlement is completed, the commerce handling process of the **Electronic Digital** Content Store(s) 100 then calls the Transaction Processor Module 175 to complete the transaction.

Transaction Processor Module 175

The role of the Transaction Processor... ...113 purchased. This information is packaged into a Transaction SC(s) 640 which is sent back to the End-User Device(s) 109 by the **Web** Server as the response to the purchase submission. The Transaction Processor Module 175 requires three pieces of information from the commerce handling process of the **Electronic Digital** Content Store(s) 103: the Product IDs for the Content 113 purchased, Transaction Data 642, and an HTML page or CGI URL acknowledging the purchase settlement.

The Product ID is the value provided to the **Electronic Digital** Content Store(s) 103 in the Metadata SC(s) 620 associated to the Content 113 just sold. This Product ID is used to retrieve the... ...SC(s) 641 from the Offer Database 181.

The Transaction Data 642 is a structure of information provided by the transaction processing function of the **Electronic Digital** Content Store(s) 103 which is later used to correlate the ClearingHouse(s) 105 processing with the financial settlement transaction performed by the **Electronic Digital** Content Store(s) 103 and to provide user identity information to be included in the watermark of the Content 113 downloaded to the End-User... ...109. When the ClearingHouse(s) 105 receives a valid Order SC(s) 650, it logs a transaction indicating the Content

113 that was sold, which **Electronic Digital** Content Store(s) 103 sold it and the associated Transaction Data 642 including the End-User's Name and a Transaction ID 535. The Transaction ID 535 provides a reference to the financial settlement transaction. This information is later returned by the ClearingHouse(s) 105 to the **Electronic Digital** Content Store(s) 103 for use in reconciling its accounts with the billing statements received from the Content Provider(s) 101 (or his agent). The Clearinghouse Transaction Log 178 can be **used** by the **Content** Provider(s) 101 to determine what Content 113 of his has been sold and enables him to create a bill to each **Electronic Digital** Content Store(s) 103 for royalties owed him. Other **electronic** means besides billing can alternatively be used to settle accounts between the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103.

The information provided in the Transaction SC(s) 640 and the security and integrity of the Transaction SC(s) 640 provide... ...the purchase transaction is valid and thus no further validation is required prior to the logging of this sale by the ClearingHouse(s) 105. The **Electronic Digital** Content Store(s) 103, however, has the option to request authentication before its accounts are charged (transaction logged at the ClearingHouse(s) 105 indicating to the Content Provider(s) 101 that this **Electronic Digital** Content Store(s) 103 has collected money for the sale of this Content 113). This request for authentication/notification is indicated by a flag in the Transaction Data 642. In this scenario, the ClearingHouse(s) 105 contacts the **Electronic Digital** Content Store(s) 103 and receive authorisation from the **Electronic Digital** Content Store(s) 103 before the charge to his account and the release of the encryption Key 623. The Transaction ID 535 is passed to the **Electronic Digital** Content Store(s) 103 from the ClearingHouse(s) 105 as part of this authentication request to enable the **Electronic Digital** Content Store(s) 103 to associate this request to a prior transaction performed with the End-User(s). This Transaction ID 535 can be any unique value the **Electronic Digital** Content Store(s) 103 wishes to use and is solely for its benefit.

The Transaction Data 642 also contains a customer name. This name can... ...of the purchase form filled out by the user when making his purchase, or from information logged previously during some user registration process with the **Electronic Digital** Content Store(s) 103, or the official name obtained from credit card information associated with the card used in this transaction. This name is later included in the **License** Watermark 527.

The Transaction Data 642 also contains the Store Usage Conditions 519 purchased by the End-User(s). This information is included in the **License** Watermark 527 and used by the End-User Device(s) 109 in Copy and Play Control.

The final parameter required by the Transaction Processor Module 175 is the HTML page or CGI URL acknowledging the purchase settlement. The purpose of

this is to allow the **Electronic Digital** Content Store(s) 103 to respond to the End-User(s) with an acknowledgement of the financial settlement and whatever other information he wishes to... ...the Transaction SC(s) 640 is received and processed.

The Transaction SC(s) 640 is the HTTP response to the End-User(s) from the **Electronic Digital** Content Store(s) 103 after processing the purchase submission. Sending a SC(s) as the direct HTTP response forces the automatic loading on the End...use by the Notification Interface Module 176 and the Account Reconciliation Tool 179.

4. Notification Interface Module 176

The Notification Interface Module 176 is a **Web** Server side executable routine (CGI or function callable by NSAPI, ISAPI or equivalent). It handles optional requests and notifications from the ClearingHouse(s) 105, the End-User Device(s) 109, the Content Hosting Site(s) 111, and the Content Provider(s) 101. The events that the **Electronic Digital** Content Store(s) 103 can optionally request notification for are:

* Notification from the ClearingHouse(s) 105 that the End-User Device(s) 109 requested an... ...ClearingHouse(s) 105 is releasing the encryption Key 623 for the specified Content 113. This notification can optionally be configured to require authentication from the **Electronic Digital** Content Store(s) 103 prior to the encryption Key 623 being sent to the End-User Device(s) 109.

* Notification from the Content Hosting Site... ...been sent to the End-User Device(s) 109.

* Notification from the End-User Device(s) 109 that the Content SC(s) 630 and the **License** SC(s) 660 have been received and successfully used to process the Content 113 or was found to be corrupt.

* Notification from the Content Provider(s) 101 that new Content 113 has been placed in the Content Promotions **Web** Site 156.

None of these notifications are a required step in the Secure **Digital** Content **Electronic** Distribution System flows 100 but are provided as options to allow the **Electronic Digital** Content Store(s) 103 the opportunity to close its records on the satisfaction of completion of the sale. It also provides information that may be needed to handle customer service requests by letting the **Electronic Digital** Content Store(s) 103 know what functions have transpired since financial settlement of the transaction or what errors occurred during an attempt to complete the... ...from the ClearingHouse(s) 105 through the Customer Service Interface 184 as needed.

Frequency of notification of new Content 113 available at the Content Promotions **Web** Site 156 is determined by the Content Provider(s) 101. Notification may be provided as each new Metadata SC(s) 620 is added or just... ...all new Metadata SC(s) 620 added that day.

All of these notifications result in entries being made to the Transaction Log 178. If the **Electronic Digital** Content Store(s) 103 wishes to perform his own processing on these notifications, he can intercept the CGI call, perform his unique function and then... ...to compare the Transaction Log 178 with the log of the ClearingHouse(s) 105. This is an optional process which is available to help the **Electronic Digital** Content Store(s) 103 feel comfortable with the accounting for the Secure **Digital** Content **Electronic** Distribution System 100.

In another embodiment, this tool can be updated to provide **electronic** funds transfers for automated periodic payments to the Content Provider(s) 101 and the ClearingHouse(s) 105. It can also be designed to automatically process payments upon reception of an **electronic** bill from the ClearingHouse(s) 105 after reconciling the bill against the Transaction Log 178.

C. Broadcast **Electronic Digital** Content Distribution Service

Broadcast primarily refers to a one to many transmission method where there is no personal interaction between the End-User Device(s) 109 and the **Electronic Digital** Content Store(s) 103 to customise on-demand viewing and listening. This is typically provided over a **digital** satellite or cable infrastructure where the Content 113 is preprogrammed so that all End-User Device(s) 109 receive the same stream.

A hybrid model can also be defined such that an **Electronic Digital** Content Store(s) 103 provides a **digital** content service organised in such a way that it can offer both a **web** distribution interface via an **Internet** connection as well as a higher bandwidth satellite or cable distribution interface via a broadcast service, with a great deal of commonality to the site design. If the IRD back -channel serial interface were connected to the **web**, and the IRD supported **web** navigation, the End-User(s) could navigate the **digital** content service in the usual way via the back-channel **Internet** interface, previewing and selecting Content 113 to purchase. The user can select high quality downloadable Content 113, purchase these selections, and receive the required **License** SC(s) 660 all via an **Internet** connection and then request delivery of the Content 113 (Content SC(s) 630) over the higher bandwidth broadcast interface. The **Web** service can indicate which Content 113 would be available for download in this manner based on the broadcast schedule or could build the broadcast streams based totally on purchased Content 113. This method would allow a **Web** based **digital** content service to contract with a broadcast facility to deliver high quality Content 113 to

users equipped with the proper equipment making a limited number... ...specific Content 113 (e.g. songs or CDS) available daily in this manner and the entire catalog available for download in lower quality via the **web** interface.

Other broadcast models can be designed where there is no **web** interface to the End-User Device(s) 109. In this model, promotional content is packaged in specially formatted **digital** streams for broadcast delivery to the End-User Device(s) 109 (i.e. IRD) where special processing is performed to decode the streams and present...End-User Device(s) 109 to the ClearingHouse(s) 105 and would utilise SC(s) to perform all data exchange. The toolset provided to the **Electronic Digital** Content Store(s) 103 has been architected and developed in such a way that most of the tools apply to both a point-to-point **Internet** service offering as well as a broadcast satellite or cable offering. The tools used by a **Digital** Content **Web** Site **Electronic Digital** Content Store(s) 103 to acquire and manage Content 113 as well as prepare SC(s) is also used by a satellite based **Electronic Digital** Content Store(s) 103 to manage and prepare Content 113 for distribution on a broadcast infrastructure. The SC(s) distributed over a **Web** service are the same as those distributed over a broadcast service.

1. Multi-Tier **Digital** TV Embodiment

Turning now to FIG. 18, shown is a high level logical diagram of an alternate embodiment of **electronic** distribution of **digital** content using broadcast infrastructure, according to the present invention. In this embodiment, the Content Provider(s) 101, as previously described above in FIG. 6, provide Metadata SC(s) 620 to one or more **Electronic Digital** Content Store(s) 103 and a Content SC(s) 630 to one or more Content Host Site(s) 111. The **Electronic** Store(s) 103 customised the Metadata SC(s) 620 to create an Offer SC(s) 641. The Offer SC(s) 641 is sent to one... ...105 through a back channel such as a telephone line.

FIG. 19 is a detailed block diagram of FIG. 18, illustrating an alternate embodiment of **electronic** distribution of **digital** content using broadcast infrastructure , according to the present invention. The Broadcast Centre(s) 1802 receive the Offer SC(s) 641. The Carousel Builder & Broadcaster 1902 creates a variety of additional broadcast content that is sent along with the broadcast stream. Techniques for transmitting **digital** information or **digital** content along with the primary broadcast stream include Intel's Intellicast system which places information in the vertical blanking interval of a standard television broadcast... ...can be sent as MPEG-2 standard transport stream for broadcast transmission and it allows the solution to be deployed over virtually all types of **digital** broadcast systems. FIG. 20 is a block diagram of the packet being broadcast in the alternate embodiment of FIG. 18, according to the present invention... ...packages 2006 mentioned above, Content SC(s) 630 and Global SC(s) 2040, and the tracks 2002 for each Content 113 is sent. In a **music** embodiment, the tracks 2002 are **musical**

tracks. The carousel format of the package format is illustrated in FIG. 20, the packages 2006 are transmitted over the broadcast infrastructure in a cyclical... ...part of the series of packets 2006 (P(underscore)1 ....P(underscore)N) is sent as part of the packet stream.

As stated above, the **digital** Content 113 is organised in packages 2006. A package 2006 is associated with a promotional material, meta-data, a package descriptor, and one (optional) video-clip . The promotional material consists of graphics and text material associated with the package **digital** content (e.g., cover art associated with a **music** album); the meta-data is a set of attributes-value pairs associated with the package (e.g., title, price, artist, etc.); a package descriptor is a set of attribute-value pairs that are used for extracting the structured **digital** content from a package (e.g., package-size and number-of-sections); the video-clip presents and promotes the content of the package in video format (e.g., a short **music** video of an artist performing a song included in the **music** album associated with the package).

The packages 2006 as well as the promotional material, the video-clip, meta-data, and a package descriptor are transmitted by a Broadcast Centre 1802 in one or more **digital** broadcast channels in a carousel fashion. A carousel is a continuous **digital** streams that repeats itself over a set of broadcast intervals. A broadcast receiver allows a user to select and download packages 2006 as well as extract the **digital** content from a package.

Packages 2006 are organised in two sets: static offering (not shown) and dynamic offering (not shown). The static offering represents the... ...provides a video decoder, a graphical user interface and receives user input. The Set-Top Box(es) 1804 allows the user to tune to a **digital** TV channel to display video clip associated with video-clip static-offering. The Set-Top Box(es) 1804 allows the user to select packages 2006... ...tunes to the carousels that contains the package and then starts collecting the data associated with the package. Package data is organisedin sections. Due to **digital** transmission errors, sections maybe corrupted and/or lost. Sections integrity is determined using CRC-32 style information. In one embodiment, the Set-Top Box(es... ...been collected and re-ordered the Set-Top Box(es) 1804 re-assembles the package. If a separate bi-directional unicast channel (such as the **Internet**) is available, the Set-Top Box(es) 1804 can use this channel to collect the missing package portion. Using the latter mechanism the package download... ...The package descriptors and the promotional material are broadcasted using a two-tier paradigm that allows for the real-time update of the receiver.

2. **Web** broadcasting Over Separate Channels Embodiment

FIG. 27 is a detailed block diagram of FIG. 18, illustrating an alternate embodiment of **electronic** distribution of **digital** content using separate channels in a **web** broadcasting service, according to the present invention. This exemplary architecture overview in FIG. 27 is used to illustrate a small number of changes that have to be made from the other embodiments for the delivery of **music** content over broadcast or telecommunications line. In particular, using current webcast infrastructure such as Hughs DirecPCTM only a few elements are added to adapt only... ...described further below on End User Device(s) 109.

As described previously, the Broadcast Centre(s) 2702 receives the Offer SC(s) 641 from the **Electronic Digital** Content Store(s) 103. Along with the Offer SC(s) 641, the corresponding Content SC(s) 630 is retrieved. In this embodiment, the Offer SC(s) 641 and the Content SC(s) 630 are stored locally on computer storage device 2704. A **web** store 2706 running CGI or servlet scripts 2708 and 2710 takes the promotional content to form sample buttons and catalog listing as are depicted and...credit cards, debit cards and other payment verification systems, an eCommerce CGI 2710 interfaces with a financial clearing house 2710. The content placed on the **Web** Store 2706 is sent to a repository 2712.

In one embodiment, the content sent to the repository is in response to user selections received via... ...for broadcast via transmitter 2716 across various channels. In one embodiment, the Server/Crawler 2714 retrieves content to be transmitted using a technique known as "**Web** crawling" in which a crawler automatically retrieves, recursively, content references via identifiers such as URLs or some other retrieval process. In another embodiment, the **Electronic Digital** Content Store(s) 103 may "push" content embodied in the Offer SC(s) 641 and the Content SC(s) 630. Once the content is assembled... ...receiver 1804. The receiver 2718 in the direct broadcast embodiment, is a USB modem coupled to a DirecPCTM or combination DirecPCTM / DirectTVTM dish or equivalent **web** cast broadcast system. A cache manager 2720 is a software program that manages the download of content and promotional materials on the End User Device... ...in the End User Device(s) 109 can be combined into one unit or implemented as separate hardware including the receiver 2718, cache manager 2720, **web** browser 191, promo cache 2722, and album + DSC(s) buffer 2724. For example, the DirecPCTM in one embodiment is housed in a set-top box... ...even when the End User Device(s) is disconnected, that is not receiving a broadcast from the transmitter 2716 and/or not communicating back the **Web** store 2706 through a back channel.

As mentioned above, the promo cache 2722 stores promotions received by the End User Device(s) 109 and similarly... ...The storage of both the promotional materials on the content locally makes the user system including the content up to date.

A user using the **Web** Browser 191, browses the promotional material previously cached in the promo cache 2722. Exemplary user interfaces are illustrated and

shown in FIG. 28 below. It... ...clip may be played through the Player Application 196 which is triggered by the trigger manager 2726. Once a user makes a selection using the **Web** Browser 191 the cache manager checks to see if the corresponding Content SC(s) 630 are available in Album+DSC Buffer 2724 and in the...the corresponding channel for downloading.

In an optional embodiment, the next time the user signs on or logon using the back channel such as the **Internet** into the Broadcast Centre(s) 2702 a confirmation of the user account information is made such as credit card payment using the e-commerce site... ...of Content 113 is accomplished by allowing user to make a certain number of purchases without reconnecting back to the ClearingHouse(s) 105 or the **Web** Store 2706. In this "off-line" embodiment, several categories may be used such as credit limits, purchase limits, periodic connection, limited time use of the... ...the download and other information useful to a user in wishing to render or play the Content 113 desired.

And as previously described for the "**online**" or "connected" version of the current delivery system, the necessary steps of updating usage conditions and **rights** associated with the Content can be monitored through the Clearing House(s) 105.

X. END-USER DEVICE(S) 109

The applications in the End-User Device(s) 109 for the Secure **Digital** Content **Electronic** Distribution System 100 perform two main functions: first the SC(s) processing and copy control; and second playback of encrypted Content 113. Whether the End-User Device(s) 109 is a Personal Computer or a specialised **electronic** consumer device, it has to be capable of performing these base functions. The End-User Device(s) 109 also provides a variety of additional features and functions like creating play lists, managing the **digital** content library, displaying information and images during content playback, and recording to external media devices. These functions vary based on the services these applications are... ...FIG.10, shown is the major components and processes and End-User Device(s) 109 Functional Flow. The applications designed to support a PC based **web** interface Content 113 service consists of two executable software applications: the SC(s) Processor 192 and the Player Application 195. The SC(s) Processor 192 is an executable application which is configured as a Helper Application into the End-User(s) **Web** Browser 191 to handle SC(s) File/MIME Types. This application is launched by the Browser whenever SC(s) are received from the **Electronic Digital** Content Store(s) 103, the ClearingHouse(s) 105, and the Content Hosting Site(s) 111. It is responsible for performing all required processing of the SC(s) and eventually adding Content 113 to the **Digital** Content Library 196 of the End-User(s).

The Player Application 195 is a stand alone executable application which the End-User(s) loads to perform Content 113 in his **Digital** Content Library 196, manage his **Digital** Content Library 196 and create copies of the Content 113 if permitted. Both the Player Application 195 and SC(s) Processor 192 applications can be... ...and browsing of Content 113 information, previewing of, for example, song clips, and selecting songs for purchase is all handled via the End-User(s) **Web** Browser 191. **Electronic Digital** Content Store(s) 103 provides the shopping experience in the same way that is offered today by many Content 113 retailing **web** sites. The difference to the End-User(s) over today's **web** based Content 113 shopping is that they may now select downloadable Content 113 objects to be added to their shopping cart. If the **Electronic Digital** Content Store(s) 103 has other merchandise available for sale in addition to the downloadable objects, the End-User(s) may have a combination of physical and **electronic** downloadable merchandise in his shopping cart. The Secure **Digital** Content **Electronic** Distribution End-User Device(s) 109 are not involved until after the End-User(s) checks out and submits his final purchase authorisation to the **Electronic Digital** Content Store(s) 103. Prior to this point, all interaction is between the **Web** Server for the **Electronic Digital** Content Store(s) 103 and the Browser 191 on the End-User Device(s) 109. This includes preview of sample **Digital** Content clips. **Digital** Content clips are not packaged into SC(s) but instead are integrated into the **web** service of the **Electronic Digital** Content Store(s) 103 as downloadable files or fed from a streaming server. The format of the Content 113 clip is not dictated by the system architecture. In another embodiment, the Player Application 195 could interact directly with the **Electronic Digital** Content Store(s) 103 or ClearingHouse(s) 105 or offline using a promotional CD.

B. Application Installation

The Player Application 195 and the Helper Application 1981 are packaged into a self installing executable program which is available for download from many **web** sites. The ClearingHouse(s) 105 acts as a central location which hosts the master download page at a public **web** site. It contains links to the locations from which the installation package can be downloaded. The installation package is available at all Content Hosting Site(s) 111 to provide geographic dispersal of the download requests. Each participating **Electronic Digital** Content Store(s) 103 can also make the package available for download from their site or may just provide a link to the master download page at the public **web** site of the ClearingHouse(s) 105.

Any End-User(s) wishing to purchase downloadable Content 113, downloads and install this package. The installation is self... ...package. It unpacks and installs both the Helper Application 198 and the Player Application 195 and also configure the Helper Application 198 to the installed **Web** Browser(s).

As part of the installation, a Public/Private Key 661 pair is created for the End-User Device(s) 109 for use in processing Order and **License** SC(s) 660. A random Symmetric Key (Secret User Key) is also generated for use in protecting song encryption keys in the **License** Database 197. The Secret User Key (not shown) is protected by breaking the key into multiple parts and storing pieces of the key in multiple... ...One product this code was introduced is in the IBM ThinkPad 770 laptop computer. Here, the tamper-resistant software was used to protect the DVD **movie** player in the computer. **Digital** Content Provider(s) such as Hollywood studios, concerned about the advent of **digital movies** and the ease at which perfect copies can be made, have insisted that **movies** on DVD disc(s) contain copy protection mechanisms. IBM's tamper-resistant software made it difficult to circumvent these copy protection mechanisms. This is a... ...hackers regarding its true operation. The latter technique is largely ad hoc, but the first two build upon well-known tools in cryptography: encryption and **digital** signatures.

C. Secure Container Processor 192

When the End-User(s) submits the final purchase authorisation to the **Electronic Digital** Content Store(s) 103 for the merchandise he has collected in his shopping cart, his **Web** Browser remains active waiting for a response from the **Web** Server. The **Web** Server at the **Electronic Digital** Content Store(s) 103 processes the purchase and performs the financial settlement and then returns a Transaction SC(s) 640 to the End-User Device(s) 109. The SC(s) Processor 192 (Helper Application 198) is launched by the **Web** Browser to process the SC(s) mime type associated with the Transaction SC(s) 640. FIG. 14 is an example of user interface screens of... ...displayed with this information and the End-User(s) is presented with options to schedule the download(s) of the Content 113 (e.g. for **music**, songs or entire albums), step 1402. The End-User(s) can select immediate download or can schedule the download to occur at a later time...at install time. This Order SC(s) 650 is sent via HTTP request to the ClearingHouse(s) 105. When the ClearingHouse(s) 105 returns the **License** SC(s) 660, the Helper Application 198 is re-invoked to process the **License** SC(s) 660. The **License** SC(s) 660 is then opened and the URL of the Content Hosting Site(s) 111 is extracted from the referenced Order SC(s) 650. The **License** SC(s) 660 is then sent to the specified Content Hosting Site 111, via http request through the Browser, requesting download of the Content SC... ...a buffer is filled, it is decrypted using the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the **License** SC(s) 660, which itself is first decrypted using the Private Key. The decrypted buffer is then passed to the Watermarking function.

The Watermarking 193 extracts the Watermarking instructions from the **License** SC(s) 660 and decrypt the instructions using the Private Key of the End-User(s). The Watermarking data is then extracted from the **License** SC(s) 660 which

includes transaction information such as the purchaser's name as registered with the **Electronic Digital** Content Store(s) 103 from which this Content 113 was purchased or derived from the credit card registration information if the **Electronic Digital** Content Store(s) 103 does not provide a registration function. Also included in the watermark is the purchase date and the Transaction ID 535 assigned by the **Electronic Digital** Content Store(s) 103 to reference the specific records logged for this transaction. The Store Usage Conditions 519 are also included to be used by... ...encrypt the Content 113 using a random Symmetric Key. Once the download and Decryption and Re-Encryption 194 process is complete, the encryption Key 623 **used** by the **Content** Provider(s) 101 to originally encrypt the Content 113 is now destroyed and the new SEAL key is itself encrypted using the Secret User Key created and hidden at installation time. This new encrypted Seal Key is now stored in the **License** Database 107.

Unlike source performed at the Content Provider(s) 101 and user Watermarking performed at the End User Device(s) 109 may need to become an industry standard to be effective. These standards are still evolving. The technology is available to allow control information to be embedded in the **music** and updated a number of times. Until such time as the copy control standards are more stable, alternative methods of copy control have been provided in the Secure **Digital** Content **Electronic** Distribution System 100 so that it does not rely on the copy control watermark in order to provide **rights** management in the consumer device. Storage and p lay/record usage conditions security is implemented utilising encrypted DC Library Collections 196 that are tied to... ...Environment. Software hooks are in place to support copy control Watermarking when standards have been adopted. Support exists today for Watermarking AAC and other encoded **audio** streams at a variety of compression levels but this technology is still somewhat immature at this time to be put to use as a sole of the original content encryption algorithm. Thus use of widely accepted and proven industry standard algorithms can be used thus further enhancing **Digital** Content Industry acceptance of the Secure **Digital** Content **Electronic** Distribution System 100.

The second purpose of this Decryption and Re-Encryption 194 process is to remove the requirement that the original master encryption Key 623, **used** by the **Content** Provider(s) 101 to encrypt this Content 113, be stored on every End-User Device(s) 109 which has **licensed** this Content 113. The encrypted master Key 623, as part of the **License** SC(s) 660, is only cached on the hard disk of the End-User Device(s) 109 for a very short time and is in... ...Encryption 194 phase has completed, greatly lessens the possibility of piracy from hackers.

Once the song has been re-encrypted, it is stored in the **Digital** Content Library 196. All metadata required for use by the Player Application 195, is extracted from the associated Offer SC(s) 641 and also stored in the **Digital** Content Library 196, step 1403. Any parts of the metadata which are encrypted, such as the song lyrics, are decrypted and re-encrypted in the same manner as described

above for the other content. The same SEAL key used to encrypt the **Content** 113 is **used** for any associated metadata needing to be encrypted.

D. The Player Application 195

1. Overview

The Secure **Digital** Content **Electronic** Distribution Player Application 195 (referred to here as the Player Application 195) is analogous to both a CD, DVD or other **Digital** Content player and to a CD, DVD, or other **digital** content storage management system. At its simplest, it performs Content 113, such as playing songs or videos. At another level, it provides the End-User(s) a tool for managing his/her **Digital** Content Library 196. And just as importantly, it provides for editing and playing of collections of content, such as songs, (referred to here as Play... ...195 is assembled from a collection of components that may be individually selected and customised to the requirements of the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103. A generic version of the player is described, but customisation is possible.

Referring now to FIG. 15 there is shown a... ...sets may be selected, based on the requirements of:

* the platform (Windows, Unix, or equivalent)

* communications protocols (network, cable, etc)

* Content Provider(s) 101 or **Electronic Digital** Content Store(s) 103

* Hardware (CD, DVD, etc)

* ClearingHouse(s) 105 technology and more.

The sections below detail the various component sets. The final section... ...no definitive layout of these components. One such layout is provided in the generic player. Based on requirements from Content Provider(s) 101 and/or **Electronic Digital** Content Store(s) and other requirements, alternate layouts are possible.

This set is grouped into subgroups, starting with the components used to present End-User Display 1510 and handle controls called End-User Controls 1511 used for such low-level functions as **audio** playback , and presentation of metadata. Next, the End-User Display Component 1510 is further divided by special

function groupings (Play-list, **Digital** Content Library), and then object-container components used for grouping and placing of those lower-level components.

Within the component listings below, any reference to... ...to a CD or other recordable medium only applies to the case where the Player Application 195 has such functionality enabled. Also note that the **term** CD in that context is a generic one, that can also represent various other external recording devices, such as MiniDisc or DVD.

FIG. 16 is... ...performing the Content 113:

. Play/Stop button

. Play button

. Stop button

. Pause button

. Skip forward button

. Skip backward button

. Volume control

. Track position control/display

. **Audio** channel volume level display and more.

Controls for the displaying metadata associated with the Content 113

. Cover Picture button

. Cover Picture object

. Artist Picture button...include (corresponding screens of an End-User Interface are shown 1601 - 1605):

Play-list of display container

. Play-list Management button

. Play-list Management window

. **Digital** Content search button

. **Digital** Content search Definition object

. **Digital** Content search Submit button

. **Digital** Content search Results object

. Copy Selected Search Result Item To Play-list button

. Play-list object (editable)

. Play-list Save button

. Play-list Play button

. Play-list Pause button

. Play-list Restart button

. Create CD from Play-list button and more.

Display of **Digital** Content Library 196

. **Digital** content library button

. **Digital** content librarian window

. **Digital** content categories button

. **Digital** content categories object

. By-artist button

. By-genre button

. By-label button

. By-category button

. Delete button

. Add-to-Play-list button

. Copy to CD button

. Song List object

. Song List display container and more Containers and Misc.

. Player window container

. **Audio** controls container

. Metadata controls container

. Metadata display container

. Toolbar container object

. Sample button

. Download button

. Purchase button

. Record button

. Player Name object

. Label/Provider/Store... ...The use of the Content 113 by the Player Applications 195 on End User Device(s) 109 is logged into a database such as the **License** Database 197. The tracking of each use of Content 113 by the Player Application 195 can be transmitted to one or more logging sites such as the Clearing House(s) 105 or Content Provider(s) 101 or **Electronic Digital** Content Store(s) 103 or any site designated and coupled to Transmission Infrastructures 107. This transmission can be scheduled at predetermined times to upload the... ...example, when duplicating or copying the Content 113 stored at the End User Device(s) 109, on to an external device such as DVD Disc, **digital** tape, flash memory, mini Disc or equivalent read/writeable removable media, the use is updates to the logging site. This may be a precondition to... ...many times the Content 113 was performed; if the Content 113 has been duplicated or copied to an authorised external device such as DVD Disc, **digital** tape or mini-Disc. In cases where there are multiple distinct users of a single Player Application 195 on the End User Device(s) 109... ...any one time and the results extrapolated. In this present embodiment, the actual usage can be measures for the users logging back onto a designated **web** site such as the **Electronic Digital** Content Store(s) 103 or Content Provider(s) 101.

4. Decryption 1505, Decompression 1506 and Playback Components 1506

These components use the keys acquired by the Copy/Play Management components to unlock the **audio** data acquired from the Data Management and Library Access components, apply the appropriate decompression to prepare it for playback, and use system **audio** services to play it. In an alternate embodiment, the **audio** data acquired from the Data Management and Library Access components may be copied to removable media such as CDS, diskettes, tapes or MiniDisks.

5. Data... ...well as handle requests for information about the stored songs.

6. Inter-application Communication Components 1508

These components are used for coordination between the Secure **Digital** Content **Electronic** Distribution Player and other applications (e.g., Browser, helper-app and/or plug-in, etc) that may invoke the Player Application 195, or that the...this diagram are required for any player, but may be replaced by specialised versions depending on such things as form of encryption or scrambling being **used**, types of **audio** compression, access methods for the Content 113 library, and more.

Above the Player Object Manager 1501 are Variable Objects 1512, which are mostly derived from... ...the Player Application 195

The following embodiment is for an example where the Player Application 195 running on End-User Device(s) 109 is an **audio** player where Content 113 is **music**. It should be understood to those skilled in the art that other types of Content 113 can be supported by the Player Application 195. A typical **audio** enthusiast has a library of CDS holding songs. All of these are available within the Secure **Digital** Content **Electronic** Distribution System 100. The set of songs that have been purchased from **Electronic Digital** Content Store(s) 103 are stored within a **Digital** Content Library 196 on his or her system. The groupings of songs that are analogous to physical CDS are stored as Play-lists. In some cases a Play-list exactly emulates a CD (e.g., all tracks of a commercially available CD has been purchased from an **Electronic Digital** Content Store(s) 103 as an on-line version of the CD and is defined by a Play-list equivalent to that of the CD). But most Play-lists is put together by End-User(s) to group songs they have stored in the **Digital** Content Libraries on their systems. However for the purposes of the ensuing discussions, an example of a custom made **music** CD is **used** when the **term** a Play-list is mentioned.

When the End-User(s) starts the Player Application 195 explicitly, rather than having it start up via invocation from the SC(s) Processor 192 Application, it pre-loads to the last Play-list that was accessed. If no Play-lists exist in the **Digital**

Content Library 196, the Play-list editor is started automatically (unless the user has turned off this feature via a preference setting). See The Play... ...of an End-User Interface 1603): When the End-User(s) has invoked the Play-list function, these are the available functions:

* Open Play-list

* **Digital** Content Librarian is invoked to display a list of stored play-lists for selection. Also see **Digital** Content Librarian below for more info.

* Edit Play-list

* Invokes the Play-list Editor (see below), primed with the current Play-list if one has... ...for more info.

* Play-list Info * Display information about the Play-list.

* Song Info

* Display information about the selected song within the Play-list.

* Visit **web** site

* Load **web** site associated with this Play-list into browser.

* Librarian

* Open the **Digital** Content Librarian window. Also see **Digital** Content Librarian below for more info. The Play-list Editor (corresponding screen of an End-User Interface 1603):

When invoking the Play-list editor, these are the End-User(s)' options:

* View/Load/Delete Play-lists

* **Digital** Content Librarian is invoked to display a list of stored Play-lists for selection of one to load or delete. Also see **Digital** Content Librarian below for more info.

* Save Play-list

* Current version of Play-list is saved in the **Digital** Content Library 196.

* Delete Song

* Currently selected song is deleted from Play-list.

* Add Song

* **Digital** Content Librarian is invoked in song-search mode, for selection of song to add to the Play-list. Also see **Digital** Content Librarian below for more info.

* Set Song Information

* Display and allow changes to information about the selected song within the play-list. This information is stored within the Play-list, and does not alter information about the song stored within the **Digital** Content Library 196. These things can be changed:

* Displayed Song Title

* End-User(s) notes about the song

* Lead-in delay on playing the song...play once, restart when done, etc)

* End-User(s) notes about this Play-list Librarian (corresponding screen of an End-User Interface 1601):

* Open the **Digital** Content Librarian window. Also see **Digital** Content Librarian below for more info.

Song Play

When a song has been prepared for play, either by invoking the Player Application 195 with the song as an argument or by selecting a song for play from a Play-list or within the **Digital** Content Librarian, these are the End-User(s)' options: (corresponding screen of an End-User Interface 1601):

* Play

* Pause

* Stop

* Skip Backward

* Skip Forward

* Adjust Volume

* Adjust Track Position

* View Lyrics

* View Credits

* View CD Cover

* View Artist Picture

* View Track Information

* View other metadata

* Visit **web** site

* Play-list

* Librarian and more.

Digital Content Librarian

The **Digital** Content Librarian can be invoked implicitly when selecting songs or Play-lists (see above) or may be opened in its own window for management of...
...Play-list

Create CD from Selected Play-list (if enabled) and more.

E. End-User Device(s) 109 in Broadcast Delivery Mode

1. Multi-Tier **Digital** TV Embodiment

An alternate embodiment of the End User Device(s) 109 using broadcast delivery is now described. Returning to FIG. 19, shown is an... ...the section associated with a desired package and re-assembles the package. The End-User Device(s) 109 allows user to store and play the **digital** content (again, the **term** "play" is used broadly). The Set-Top Box(es) 1804 is a single logical module; it may be realised in separate software modules, which may... ...to the user and request the selection of a specific interval.

At the scheduled download time, the Set-Top Box(es) 1804 tunes to the **digital** channel specified in bug catalog, and begins filtering the desired package sections

out of the multiplexed broadcast stream. The Set-Top Box(es) 1804 detects...Content Host Emulator 1912 allows the same Player Application 191 to be used in this broadcast infrastructure or in a telecommunications infrastructure (such as the **Internet**) or in a computer readable medium. The Player Application 191 and associated parts including Secure Container Processor 191, Helper Application 193, Water Marking 193 and... ...It should be understood to those skilled in the art, that the broadcast embodiment of the present invention, allows for:

* Fast and reliable download of **digital** content over **digital** television broadcast infrastructure (where the **digital** content is a package, to be downloaded as a unit for later play; "play" being used broadly to refer to any form of ingest and interpretation);

* Self-contained description of the **digital** content over the **digital** television broadcast infrastructure. This system allows for the download of **digital** content over **digital** television broadcast infrastructure when a return channel from the content receiver to the content sender is not available (or infrequently available);

* Improved download time when a return channel from the content receiver to the content sender is available;

* Users to select and download **digital** content using a **digital** Set-Top Box(es) 1804 and a TV connected to the **digital** television broadcast infrastructure;

* Users to select and download **digital** content while simultaneously watching a video program;

* Content Providers to promote the **digital** content, available for download, using graphics and video;

* Managers to update, in real-time, the number and type of **digital** content available for download;

2. **Web** broadcasting Over Separate Channels Embodiment

An alternate embodiment of the End User Device(s) 109 using separate channels in a **web** broadcasting service, according to the present invention broadcast delivery is now described. Returning to FIG. 27, shown is an alternate embodiment for receiving Content 113 using separate channels in a **web** broadcasting infrastructure. FIG. 28 is a flow diagram 2800 for a process running on the End User Device for purchasing content over the alternate embodiment of FIG. 27, according to the present invention. The Set-Top Box(es) 1804 receives

web pages composed by the **Web** Store 2306 such as the exemplary illustrations of the user screens shown in FIGS. 29-38 below.

The following is a description using the flow... ...28 with reference to the exemplary user screens of FIGs. 29-38. The process begins in step 2802 with promotional material being downloaded over a **web** cast channel to a promo cache 2322. In the event the user selects the button labelled "Album List"a selection list as show in FIG... ...a selection such as "Madonna" more information is presented about the artist in FIG. 30, step 2810. Note the possibility of previewing samples of the **music** with the "Sample" buttons. When a user selects the "Sample" button a promotional clip is played through the **Web** browser 191 or alternately through Player Application 191. If the user selects to purchase a selection a screen is presented to verify the "Account" and "Password" in FIG. 31, steps 2812 and 2814. In this example, the account information can be synchronised back with the **Web** Store 2306 or synchronised latter with the ClearingHouse(s) 105 as decided by the provider of the Content 113. The cache manager 2320 examines the... ...the corresponding Content SC(s) 630 is not available, the cache manager 2320 subscribes to the next Content SC(s) 630 broadcast. Returning to the **music** example, the broadcast and download is the "Madonna Material Girl" selection. A screen with additional optional information is presented to the user once the cache... ...and times as shown in FIG. 32.

In the event the user selects "My Selections" a list of selections schedule to be downloaded via the **web** broadcast by the cache manager 2320 is shown as illustrated in FIG. 33 and steps 2816 and 2818. In this example the user repeats the... ...uses the Content 113 as described previously for the "connected" embodiments. In one embodiment, the Player Application 195 uses a back channel such as the **Internet**, to reconcile account information with the ClearingHouse(s) 105. FIG. 38 is an example of the "Madonna" title being added to a library 196 on the End User Device(s) 109. The **License** SC(s) 147 can be transmitted to the End User Device(s) 109 using any computer readable medium including the **Internet** or other telecommunications network, broadcast or via a physical mailer such as a diskette, DVD, smart card, debit card, or CD. The process flow 2800 ends with step 2830.

It should be understood that in this **web** broadcasting over separate broadcast channel embodiment, that the user does not have to be connected to order and browse promotional materials such as Offer SC...

Country	Number	Kind	Date

Legal Status Type	Pub. Date	Kind	Text

Language

Fulltext Availability	Available Text	Language	Update	Word Count
Total Word Count (Document A)				
Total Word Count (Document B)				
Total Word Count (All Documents)				

Specification: ...peculiar to an apparatus forming the home network 5, and information corresponding to the ID such as whether or not connection is possible with the **electronic** distribution service center 1, whether or not settlement processing is possible, whether or not contents can be purchased, which apparatus performs the settlement processing, which... ...are performed by this group unit. Therefore, in principle, a representative apparatus in the group collectively performs communication, settlement processing and information update with the **electronic** distribution service center 1, and other apparatuses in the group do not directly communicate with the **electronic** distribution service center 1. The ID recorded in the user registration database is the ID allocated to each apparatus separately and is used for identifying an apparatus.

Information on whether or not connection with the **electronic** distribution service center 1 recorded in the user registration database is possible indicates whether or not it possible to physically connect with the **electronic** service center 1, and even an apparatus recorded as capable of connecting, other than an apparatus recorded as capable of performing settlement processing, cannot be connected to the **electronic** distribution service center 1 in principle. (However, if a representative apparatus in a group does not perform settlement processing operation due to some reason, an apparatus can be temporarily connected to the **electronic** distribution service center 1 as a proxy.) In addition, an apparatus recorded as not capable of connecting outputs charge information or the like to the **electronic** distribution service center 1 via an apparatus capable of performing settlement processing of the user home network 5.

Information on whether or not the settlement... ...settlement. When the user home network 5 is composed of a plurality of apparatuses that are capable of performing purchase or the like of utilization **right** of contents, one apparatus that can perform settlement processing among the apparatuses transmits charge information, price information, if necessary, and a handling policy of all the apparatuses registered in the **electronic** distribution service center 1 of the user home network 5 to the **electronic** distribution service center 1, and receives the delivery key Kd)) and the registration information from the **electronic** distribution service center 1 according to the completion of the settlement processing. In this way, processing of the **electronic** distribution service center 1 is reduced compared with performing processing for each apparatus.

Information on whether or not purchase processing recorded in the user registration database indicates whether or not the apparatus can purchase the utilization **right** of contents. An apparatus that is incapable of purchasing obtains the utilization **right** of the contents by performing proxy purchase (this means that another apparatus purchases the **right** and all the **right** is assigned. No **right** remains in the supplier side) of the utilization **right** from another apparatus capable of purchasing, re-distribution (this means a method in which the utilization **right** of contents already purchased is purchased again with identical contents of the utilization **right** or different contents of the utilization **right** and supplied to another apparatus. In this case, no **right** remains in the supplier side. Main purpose of re-distribution is to make a discount. The privilege of discount is granted on condition that an apparatus belongs to a group that uses an identical settlement ID. This is because processing burden of the **electronic** distribution service center 1 is reduced in processing within the group using the identical settlement ID, and therefore a discount is granted in return), or management transfer (although a content reproduction **right**, particularly an indefinite reproduction **right** can be transferred, which apparatus is a reproduction **right** receiver is managed in a reproduction **right** transmitter, and when the reproduction **right** is not returned, the management transfer cannot be performed at all again, and the reproduction **right** can only be returned to the reproduction **right** transmitter that gave the reproduction **right**).

Here, a utilization method/a utilization **right** and purchase method of contents will be briefly described. As a utilization method of contents, there are two methods, namely a method in which a user itself manages and maintains the utilization **right** of contents, a method in which a user executes the utilization **right** held by another apparatus and utilizes the **right** in the user' s own apparatus. As the utilization **right** of contents, there are an unlimited reproduction **right** (a **right** without any limit on a period and the number of times of reproduction of contents; if the contents is **music** contents, the reproduction is sound reproduction, and if the contents is a game program or the like, the reproduction is execution), a reproduction **right** with limited number of times (a **right** with the number contents can be reproduced is limited), an unlimited copying **right** (a **right** without any limit on a period and the number of times of copying contents), a copying **right** with limited number of times (a **right** with limit on the number of times of copying contents) (as a copying **right**, there are a copying **right** without copy management information, a copying **right** with copy management information (SCMS), other copying **rights** for special purpose media, and the like) (in addition, in some cases, there is a copying **right** with a limit of time), and a management transfer **right**. As a method of purchasing the utilization **right**, there are utilization **right** content change for changing contents of the utilization **right** already purchased to other contents, re-distribution for separately purchasing the utilization **right** based on the **right** already purchased by another apparatus, proxy purchase for having another apparatus to purchase the utilization **right** on behalf of the user's apparatus, album purchase for collectively purchasing and managing a plurality of contents utilization **rights**, and the like in addition to ordinary purchase for directly purchasing the abovementioned utilization **rights**.

Information written in a proxy settler recorded in the user registration database indicates an ID of an apparatus which is made to transmit charge information generated when the

utilization **right** of contents is purchased to the **electronic** distribution service center 1 on behalf of the user's apparatus.

In formation written in a proxy purchaser recorded in the user registration database indicates an ID of an apparatus which performs purchase of the utilization **right** on behalf of an apparatus that is incapable of purchasing the utilization **right** of contents. However, if all the apparatuses within the group that can perform purchase processing are appointed as proxy purchasers, it is not specifically necessary... ...In addition, in some cases, utilization of purchased contents is also limited. (However, an apparatus may be registered again after it is brought in the **electronic** distribution service center 1 or the like and completed inspection.) In addition, a state such as "settlement unprocessed," "temporary suspension" or the like may exist...of functions of the content provider 2. The content server 31 stores contents to be supplied to a user, and supplies the contents to an **electronic** watermark adding section 32. The **electronic** watermark adding section 32 inserts a content provider ID in the contents supplied from the content server 31 in the form of an **electronic** watermark indicating the contents are properties of the user, and supplies the contents to a compression section 33. The compression section 33 compresses the contents supplied from the **electronic** watermark adding section 32 by the method of ATRAC (Adaptive Transform Acoustic Coding) (trademark) or the like, and supplies the contents to a content encryption... ...encryption section 36 encrypts the content key Kco)) by a common key encryption method such as DES using the individual key Ki)) supplied from the **electronic** distribution service center 1, and outputs the results to the signature generation section 38. Incidentally, the encryption method is not limited to DES, and a...38 corresponding to contents to be encrypted. Further, in some cases, the handling policy generation section 37 supplies the generated a handling policy to the **electronic** distribution service center 1 via communicating means (not shown), and the data is maintained and managed. The signature generation section 38 adds an **electronic** signature to the encrypted content key Kco)), the encrypted individual key Ki)) and the handling policy, and transmits them to the service provider 3 together... ...content provider 2. (The encrypted contents, the encrypted content key Kco)), the encrypted individual key Ki)) and the handling policy to each of which the **electronic** signature is added using a secret key of the content provider 3 are hereinafter referred to as a content provider secure container.) Further, one signature may be added to entire data instead of adding a signature separately to respective data.

A mutual authentication section 39 mutually authenticates with the **electronic** distribution service center 1, and mutually authenticate with the service provider 3 prior to transmitting the content provider secure container to the service provider 3... ...an elliptical curve encryption that is a public key encryption method. The processing will be described with reference to Figure 10 (EC-DSA (Elliptic Curve **Digital** Signature Algorithm), IEEE P1363/D3). In step S1, M is a message, p is a characteristic, a and b are coefficients of an elliptic curve...of the content provider 2 with respect to the handling policy stored in the content server 41 is verified using the public key of the **content** provider 2 that is ...a tamper resistant memory (not shown) (as in 40A of the content provider 2) (the content provider secure container and the price information with an **electronic** signature added using the secret key of he service provider 3 are hereinafter

referred to as a service provider secure container). Further, one signature may...
...provider 3 are supplied to the user home network 5 via the network 4 (Figure 1). A mutual authentication section 46 mutually authenticates with the **electronic** distribution service center, and if possible, mutually authenticates with the user home network 5 via the content provide, the **Internet**, cable communication or the like, if necessary.

Figure 15 is a block diagram showing a configuration of the user home network 5. A home server 51 receives a secure container containing contents from the service provider 3 via the network 4, purchases the utilization **right** of the contents, and performs decryption, extension, reproduction and copying of the contents by executing the **right**.

The communication section 61 communicates with the service provider 3 or the **electronic** distribution service center 1 via the network 4, and receives or transmits predetermined information. An upper controller 62 receives a signal from inputting means 63, displays a predetermined message or the like on displaying means 64, performing utilization **right** purchase processing or the like by utilizing an encryption processing section 65, supplies encrypted contents read out from mass storage section 68 to an extension... ...or the like, if necessary, ad may be united as one means. The encryption processing section 65 mutually authenticates with the service provider 3, the **electronic** distribution service center 1 or encryption processing sections of other apparatuses, purchases the content utilization **right**, and at the same time, performs encryption/decryption of predetermined data, manages an external memory that holds the content key Kco)) and **licensing** conditions information, and further stores the delivery key Kd)), the charge information or the like. The extension section 66 mutually authenticates with the encryption processing... ...from the upper controller 62 using the content key Kco)), extends the contents by a predetermined method such as ATRAC, and further inserts a predetermined **electronic** watermark in the contents. The external memory 67 is composed of a nonvolatile memory such as a flash memory or a nonvolatile memory with a back-up power source, and stores the content key Kco)) decrypted by the save key Ksave)) and the **license** conditions information. The mass storage section 68 is a storage device such as an HDD or an optical disk, which stores the content provider secure... ...and the signatures on them), the public key certificate, the registration information or the like.

The encryption processing section 65 for mutually authenticating with the **electronic** distribution service center 1, purchasing the content utilization **right** and, at the same time, generating the charge information, performing decryption/encryption of predetermined data, managing an external memory holding the **content** key Kco)) and the **license** conditions information, and further storing the delivery key Kd)), the charge information or the like is composed of a control section 91, a storage module... ...not to accept the charge information, whether or not to perform re-distribution or the like of the contents. The purchase processing module 94 generates **license** conditions information anew from the handling policy and the price information (as well as already holding **license** conditions information depending on a case) included in the secure container received from the ...the control section 91, and generates charge information to output to the storage module 92. The mutual authentication module 95 executes mutual

authentication with the **electronic** distribution service center 1, the encryption processing sections of other apparatuses in the home network 5 and the extension section 66, and generates a temporary... ...encrypted by the individual key Ki)), and decrypts various kinds of data encrypted by the temporary key Ktemp)). The encryption unit 112 encrypts the decrypted **content** key Kco)) by the save key Ksave)) held in the storage module 92 to output to the external memory control section 97 via the control... ...67 is divided into N blocks of data regions, and each data region is made such that M sets of content key Kco)) and the **license** conditions information can be written. In addition, other regions that can be used freely are also prepared in the external memory 67. The hash value... ...the external memory will be described later using a flowchart.

The extension section 66 (Figure 15) for decrypting and extending contents and adding a predetermined **electronic** watermark is composed of a mutual authentication module 101, a key decryption module 102, a decryption module 103, an extension module 104, an **electronic** addition module 105 and a storage module 106. The mutual authentication module 101 mutually authenticates with the encryption processing section 65, and outputs the temporary... ...output to the extension module 104. The extension module 104 further extends the decrypted contents with a method such as ATRAC to output to the **electronic** watermark addition module 105. The **electronic** watermark addition module 105 inserts to the contents the individual ID of the encryption processing section to which the purchase processing has been applied using the **electronic** watermark technology to output to other apparatuses or a speaker (not shown), and reproduces **music**.

Key data required for the mutual authentication with the encryption processing section 65 is stored in the storage module 106. Further, the extension section 66 is desirably provided with the tamper resistant feature.

The external memory 67 stores the **license** conditions information generated when the **right** is purchased in the purchase processing module 94 and the **content** key Kco)) encrypted by the save key Ksave)). The mass storage section 68 records the secure container, the public key certificate, the registration information or...memory 67, its description is omitted. The recording medium 80 is, for example, an MD (Mini Disk: trademark) or a storage medium exclusively used for **electronic** distribution (Memory Stick using a semiconductor memory: trademark).

A portable apparatus 53 that is carries by a user to reproduce and enjoy **music** is composed of a communication section 81, an upper controller 82, an encryption processing section 83, an extension section 84 and an external memory 85... ...and may be any memory such as an HDD and a rewritable optical disk.

Figure 17 illustrates a configuration of the recording media exclusively for **electronic** distribution. A recording medium 120 for storing electronically distributed contents is composed of a communication section 121, the encryption processing section 122, and the external... ...the fixed apparatus 52 (Figure 15). Since the encryption processing section 122 for mutually authenticating with the fixed apparatus 52, being assigned the content utilization **right**, performing decryption/encryption of predetermined data,

managing the external memory holding the content key Kco)), the **license** conditions information and the like, and storing the save key Ksave)) or the like has a configuration having the same function as the encryption processing... ...is omitted. The external memory 123 stores the content key Kco)) encrypted by the save key Ksave)), contents encrypted by the content key Kco)), the **license** condition information providing conditions for use of the contents, a handling policy, if necessary, and price information.

The recording media exclusively for **electronic** distribution 120 has a method of using different from the recording medium described for the fixed apparatus 52. While the ordinary recording medium 80 is a substitute for the mass storage section 68, the recording medium exclusively for **electronic** distribution 120 is not different from a portable apparatus that does not have the extension section. Therefore, although an apparatus such as the fixed apparatus 52 having the extension section 74 is necessary when reproducing contents, the recording medium exclusively for **electronic** distribution 120 can perform processing similar to that of the home server 51 or the portable apparatus 53 concerning the function for managing the contents... ...medium 80 cannot be reproduced by an apparatus other than the one that has recorded the same, contents recorded in the recording medium exclusively for **electronic** distribution 120 can be reproduced by an apparatus other than the one that has recorded the same. That is, since the ordinary recording medium 80... ...by an apparatus other than the one that has (has recorded) the content key Kco)). On the other hand, since the recording medium exclusively for **electronic** distribution 120 retains not only the contents encrypted by the content key Kco)) but also the content key Kco)) encrypted by the save key Ksave)) peculiar to the recording medium exclusively for **electronic** distribution, the contents can be reproduced by other apparatuses.

That is, after performing mutual authentication between the mutual authentication module 128 of the encryption processing section 122 and the mutual authentication module (not shown) of the encryption processing section 73, the recording medium exclusively for **electronic** distribution 120 decrypts the content key Kco)) by the save key Ksave3)), encrypts the content key Kco)) by the shared temporary key Ktemp)) to transmit... ...be unnecessary because it is in the registration information), a secret key different for each apparatus, the save key Ksave)), the public key of the **electronic** distribution service center 1 to be used when mutually authenticating with the **electronic** distribution service center 1 (unnecessary if there is the public key certificate of the **electronic** distribution service center 1), the public key of the authentication station 22 for verifying the public key certificate, and the common key to be used... ...data that are stored in advance when an apparatus is manufactured. On the other hand, the delivery key Kd)) to be periodically distributed from the **electronic** distribution service center 1, the charge information to be written upon the purchase processing, the content key Kco)) held in the external memory 67, and the hash value for tamper checking of the **license** conditions information are data that are stored after starting use an apparatus, and are also stored in the storage module 92. The individual ID for...the extension section 66.)

The content key Kco)) that is encrypted by the save key Ksave)) to be used when contents are decrypted, and the **license** conditions information indicating conditions for

utilizing the content key Kco)) are stored in the external memory 67. In addition, the certificate (the public key certificate... ...the individual ID for specifying an apparatus, the secret key that is different for each apparatus, the save key Ksave)), the public key of the **electronic** distribution service center 1 to be used when mutually authenticating with the **electronic** distribution service center 1 (however, it is not necessary to have the home server 51 to perform all the procedures with the **electronic** distribution service center 1 on its behalf), the public key of the authentication station 22 for verifying the public key certificate, and the common key... ...that are stored in advance when an apparatus is manufactured. In addition, the hash value for checking tamper of the content key Kco)) and the **license** conditions information to be retained in the external memory 85, the ID for settlement, if necessary, the delivery key Kd)), and (a part of) the... ...information and its signature are also stored) , the content key Kco)) encrypted by the save key Ksave)) to be used for decrypting the contents, the **license** conditions information indicating conditions for utilizing the contents are stored in the external memory 85. A public key certificate for the content provider 2 and... ...of the home server 51. The recording medium 80 may be an ordinary MD or CD-R, or may be a storage medium exclusively for **electronic** distribution. In the former case, although data to be stored is decrypted contents with a copy prohibit signal added, encrypted contents may be naturally included... ...the save key Ksave)) is different for each apparatus.)

In addition, as the storage medium, Figure 19 is possible. In the storage medium exclusively for **electronic** distribution 120, the individual ID of the recording medium, the secret key different for each recording medium, the public key certificate corresponding to the secret key (which may be recorded in the external memory 123), the save key Ksave)) to be **used** for encrypting the content key Kco)) (which are generally different for each storage medium), the public key of the **electronic** distribution service center 1 (which is not required if there is not communication with the center or if the public key certificate of the **electronic** distribution service center 1 exists in the external memory 123), the public key of the authentication station, the hash value for inspecting tamper of the... ...125 in the encryption processing section 122. The contents encrypted by the content key Kco)) (and its signature), and the content key Kco)) and the **license** conditions information encrypted by the save key Ksave)) are stored in the external memory 123, and the handling policy (and ...the service provider 3 are also stored, if necessary.

Figures 20 and 21 are drawings for illustrating information to be transmitted and received among the **electronic** distribution service center 1, the content provider 2, the service provider 3, and the user home network 5. The content provider 2 adds the public... ...provider 3. In addition, the content provider 2 transmits the handling policy and its signature, and the certificate of the content provider 2 to the **electronic** distribution service center 1, if necessary.

The service provider 3 verifies the public key certificate of the content provider 2, obtains the public key of... ...In addition, the service provider 3 transmits the price information and its signature, and the public key certificate of the service provider 3 to the **electronic** distribution service center 1, if necessary.

After verifying the received secure containers, the user home network 5 performs the purchase processing based on the handling... ...the price information included in the secure containers, generates the charge information to store in the storage module in the encryption processing section, generates the **license** conditions information, decrypts the content key Kco)) and re-encrypts the same by the save key Ksave)), and stores the **license** conditions information and the re-encrypted content key Kco)) in the external memory 67. Then, the user home network 5 decodes the content key Kco)) by the save key Ksave)) along the **license** conditions information, and decrypts the contents by the key to utilize. The charge information is encrypted by the temporary key Ktemp)) at a predetermined timing, added a signature, and transmitted to the **electronic** distribution service center 1 together with the handling policy and the price information, if necessary.

The **electronic** distribution service center 1 calculates usage fees based on the charge information and the price information, and calculates profits of each of the **electronic** distribution service center 1, the content provider 2 and the service provider 3. The **electronic** distribution service center 1 further compares the handling policy received from the content provider 2, the price information and the handling policy, if necessary, received... ...tampering of the handling policy or illegal addition of prices has occurred in the service provider 3 or the user home network 5.

Moreover, the **electronic** distribution service center 1 transmits the public key certificate of the content provider to the content provider 2, and transmits the public key certificate of... ...addition, since the public key certificate prepared according to each apparatus is embedded in each apparatus when the apparatus is shipped from a factory, the **electronic** distribution service center 1 transfers the data concerning the public key certificate of each apparatus to the factory.

Figure 22 illustrates the content provider secure...be allocated to the user apparatus (more precisely the encryption processing section (a exclusive use ticket)) by the authentication station, an algorithm and a parameter **used** for the signature, a name of the authentication station, an effective period of the public key certificate, a name of the user apparatus, the public... ...of a handling policy that is generated for each single content or album content by the content provider 2 and shows contents of a utilization **right** purchasable by the user home network 5.

In the data of the handling policy for the single content (Figure 33), a type of the data... ...regional code, usable apparatus conditions, usable user conditions, an ID of the service provider, generation management information, the number of rules including the purchasable utilization **right** indicated by the handling policy, address information indicating the storage position of the rules, the rules stored in the position indicated by the address information, the public key certificate and signatures.

The rule is composed of a rule number given as a serial number for each utilization **right**, a utilization **right content** number indicating the utilization **right** contents, its parameter, a minimum sales price, a profit amount of the content provider, a profit ratio of the content provider, a data size, and... ...policy of the single content stored in the position

indicated by the address information, generation management information, the number of rules including the purchasable utilization **right** indicated by the handling policy, address information indicating the storage position of the rules, the rules stored in the position indicated by the address information... ...rule of the handling policy of the single content, the rules is composed of a rule number given as a serial number for each utilization **right**, a utilization **right** content number indicating the utilization **right** contents, its parameter, a minimum sales price, a profit amount of the content provider, a profit ratio of the content provider, a data size, and...signature and a key to be used for verification of the signature are included in the public key certificate. In addition, in rules, a utilization **right** content number is a number added for each utilization **right** content, and a parameter indicates a parameter of **right** contents. A minimum sales price indicates a minimum sales price in selling single or album contents according to the utilization **right** contents, a profit amount and a profit ratio of a content provider indicates an amount of a profit that a content provider 2 can obtain... ...data size of transmission information, and the transmission information consists of a point to be added to a user through a purchase of the utilization **right** set by the content provider 2, mileage information made up of a discount amount of the utilization **right** according to the point, and various kinds of information set by the content provider 2, if necessary.

Here, in the handling policy of the album... ...handling policy of single and album contents, since a profit amount and a profit ratio of a content provider can be managed altogether by the **electronic** distribution service center 1, the handling policy can be formed excluding the profit amount and the profit ratio of the content provider.

Figures 37 and... ...of the content provider, an ID of the handling policy to which the price information is added, the number of rules including the purchasable utilization **right** indicated by the price information, address information indicating the storage position of the rules, the rules stored in the position indicated by the address information, the public key certificate and signatures.

The rule is composed of a rule number given as a serial number for each utilization **right**, a profit amount of the service provider, a profit ratio of the service provider, a price, a data size, and transmission information.

In addition, in single contents stored in the position indicated by the address information, the number of rules including the purchasable utilization **right** indicated by the price information, address information indicating the storage position of the rules, the rules stored in the position indicated by the address information... ...rule of the price information for the single contents, the rule is composed of a rule number given as a serial number for each utilization **right**, a profit amount of the service provider, a profit ratio of the service provider, a price, a data size, and transmission information.

In the above... ...the price indicates a sales price of the single contents and the album contents that are set by the service provider 3 based on utilization **right** contents and a corresponding minimum sales price. A data size indicates data size of transmission information, and the transmission information consists of a point to be added to a user

through a purchase of the utilization **right** set by the service provider 3, mileage information made up of a discount amount of the utilization **right** according to the point, and various kinds of information set by the service provider 3, if necessary.

Here, when generating price information, the service provider 3 can set all the purchasable utilization **right** indicated by a corresponding a handling policy as a purchasable **right** indicated by the price information, and at the same time, can set a utilization **right** arbitrary selected out of all the purchasable utilization **right** indicated by the handling policy, thus, can select a utilization **right** provided for by the content provider 2.

In addition, in price information of album contents, a plurality of rules provides for a sales price corresponding amount and a profit ratio of a service provider can be managed altogether by the **electronic** distribution service center 1, the price information may be formed excluding the profit amount and the profit ratio of the service provider.

Figure 41 illustrates a data format of **license** conditions information, and the **license** conditions information is prepared, when a user purchases contents, based on a handling policy of the purchased contents in an apparatus in the user home network 5, and indicates utilization **right** contents selected by the user among utilization **right** contents indicated by the handling policy.

In data of **license** conditions information, a type of data, a type of **license** conditions information, an effective period of the **license** conditions information, an ID of contents, an ID of an album, an ID of an encryption processing section, an ID of a user, an ID... ...policy, version of the handling policy, an ID of a service provider, an ID of price information, a version of price information, an ID of **license** conditions information, a rule number attached to a reproduction **right** (utilization **right**) as a serial number, a utilization **right** content number, a remaining number of time of reproduction, an effective period of the reproduction **right**, a rule number attached to a copying **right** (utilization **right**) as a serial number, a utilization **right** content number, a remaining number of times of copying, generation management information, and an ID of an encryption section having a reproduction **right** are stored.

In **license** conditions information, a type of data indicates that the data is data of the **license** conditions information, a type of **license** conditions information indicates whether the **license** conditions information is **license** conditions information of single contents or album contents. An effective period of **license** conditions information indicates a usage period of the **license** conditions information by a data when the period expires, the number of days from a day to be a basis of start using until a... ...addition, an ID of a content provider indicates an ID of a content provider 2 that has provider for a handling policy used for preparing **license** conditions information, and an ID of a handling policy indicates a handling policy used for preparing the **license** conditions information. An version of a handling policy indicates revision information of a handling policy used for preparing **license** conditions information. An ID of a service provider indicates an ID of a service provider 3 that has prepared price information used for preparing **license**

conditions information, and an ID of price information indicates price information used for preparing the **license** conditions information. A version of price information indicates revision information of a handling policy used for preparing **license** conditions information. Therefore, a content provider 2 or a service provider 3 that has provided contents purchased by a user can be found by the... ...version of a handling policy, the ID of a service provider, the ID of price information and the version of price information.

An ID of **license** conditions information is attached by an encryption processing section of an apparatus in a user home network 5 that has purchased contents, and is used for identifying the **license** conditions information. A rule number of a reproduction **right** indicates a serial number attached to a reproduction **right** among a utilization **right**, and uses a rule number of a rule indicated by a corresponding handling policy or price information as it is. Utilization **right** contents indicate contents of a reproduction **right** to be described later. A remaining number of times of reproduction indicates a remaining number of times of reproduction among a number of times of reproduction set in advance to contents, and an effective period of a reproduction **right** indicates a corresponding reproduction available period of purchased contents by a date and time when the period expires.

In addition, a rule number of a copying **right** indicates a serial number attached to a copying **right** among a utilization **right**, and uses a rule number of a rule indicated by a corresponding handling policy and price information as it is. Utilization **right** contents indicate contents of a copying **right** to be described later. A remaining number of times of copying indicates a remaining number of times of copying among a number of times of... ...contents are re-purchased, a remaining number of times the contents can be re-purchased. An ID of an encryption processing section having a reproduction **right** indicates an encryption processing section having a reproduction **right** at the current time, and when management is shifted, an ID of an encryption processing section having a reproduction **right** is changed.

Incidentally, in **license** conditions information, an effective period may be provided for with respect to a copying **right**, and when the effective period is provided for, a period for purchased contents in which copying is available is indicated by a date and time... ...a version of a handling policy, an ID of a service provider, an ID of price information, a version of price information, an ID of **license** conditions information, a rule number, a profit amount and a profit ratio of a content provider 2, a profit amount and a profit ratio of... ...indicates price information used for the purchase processing. A version of price information indicates revision information of price information used for purchase processing.

An ID of **license** conditions information indicates an ID of **license** conditions information that has been prepared upon purchase processing, and a rule number indicates a rule number attached to a purchased utilization **right** as a serial number. A profit amount and a profit ratio of a content provider indicate an amount of dividend that is distributed to a... ...a profit ratio of a content provider and a profit amount and a profit ratio of a service provider may be managed altogether by the **electronic** distribution service center 1, the

charge information may be formed excluding the profit amount and the profit ratio of the content provider as shown in Figure 43.

Figure 44 shows contents of a purchasable utilization **right**, and as the utilization **right**, there are roughly a reproduction **right**, a copying **right**, a **right** content changing **right**, a re-purchase **right**, an additional purchase **right**, and a management transfer **right**.

The reproduction **right** includes an unlimited reproduction **right** that does not have limitations on a period or the number of times of reproduction, a reproduction **right** with a period limitation that limits a reproduction period, a reproduction **right** with a cumulating time limitation that limits cumulating time of reproduction, and a reproduction **right** with a number of times limitation that limits the number of times of reproduction. The copying **right** includes an unlimited copying **right** without a period limitation, a number of times limitation and copy management information (e.g., the serial copy management: SCMS), a copying **right** with a number of times limitation and without copy management information that limits the number of times of copying but does not have copy management information, a copying **right** with copy management information that does not have a period limitation and a number of times limitation but adds and provides copy management information, and a copying **right** with a number of times limitation and copy management information that limits the number of times of copying, and adds and provides copy management information. Incidentally, in addition to the above, as a copying **right**, there are a copying **right** with a period limitation that limits a copy available period (including the one that adds copy management information and the one that does not add the copy management information) , and a copying **right** with a cumulating time limitation that limits a cumulating time of copying (i.e., a cumulating time ...including the one that adds copy management information and the one that does not add the copy management information), and the like.

In addition, the **right** contents changing **right** is a **right** for changing contents of a **right** already purchased to other contents, and the re-purchase **right** is a **right** for separately purchasing a utilization **right** based on a **right** purchased by other apparatuses as described above . The additional purchase **right** is a **right** for purchasing and adding to independently purchased contents other contents of an album including the contents, and the management transfer **right** is a **right** for transferring a purchased **right** to change an owner.

An specific example of utilization **right** contents shown in Figure 33, etc. will now be described. In fact, as shown in Figure 45A, as data of the unlimited reproduction **right**, information on an effective period of a reproduction **right** that indicates an effective period of a reproduction **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period until a date on which the period expires, or the like is stored in a region of utilization **right** contents. As shown in Figure 45B, as data of the reproduction **right** with a period limitation, information on an effective period of the reproduction **right** that indicates an effective period of a reproduction **right** by a date on which the period expires, or the number of days from a

date to be a basis of starting an effective period until a date on which the period expires, or the like is stored in a region of utilization **right** contents.

As shown in Figure 45C, as data of the reproduction **right** with a cumulating limitation, information on an effective period of the reproduction **right** that indicates an effective period of a reproduction **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period... ...information on the number of days and time indicating a limitation of accumulating time contents can be reproduced are stored in a region of utilization **right** contents. As shown in Figure 45D, as data of the reproduction **right** with a number of times limitation, information on an effective period of the reproduction **right** that indicates an effective period of a reproduction **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period... ...and information on the number of times of reproduction indicating the number of times contents can be reproduced are stored in a region of utilization **right** contents.

In addition, as shown in Figure 45E, as data of the unlimited copying **right** without copy management information, information on an effective period of the copying **right** that indicates an effective period of a copying **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period until a date on which the period expires, or the like is stored in a region of utilization **right** contents. As shown in Figure 45F, as data of the copying **right** with a number of times limitation and without copy management information, information on an effective period of the copying **right** that indicates an effective period of a copying **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period... ...information on the number of times of copying that indicates the number of times contents can be copied are stored in a region of utilization **right** contents.

In addition, as shown in Figure 45G, as data of the copying **right** with copy management information, information on an effective period of the copying **right** that indicates an effective period of a copying **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period until a date on which the period expires, or the like is stored in a region of utilization **right** contents. As shown in Figure 45H, as data of the copying **right** with a number of times limitation and copy management information, information on an effective period of the copying **right** that indicates an effective period of a copying **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period... ...information on the number of times of copying that indicates the number of times contents can be copied are stored in a region of utilization **right** contents.

Moreover, as shown in Figure 45I, as data of the **right** contents changing **right**, information on an effective period of the **right** contents changing **right** that indicates an effective period of a **right** content changing **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period until a date on which the period expires, or the like, an old rule number for retrieving utilization **right** contents before change, and a new rule number for retrieving utilization **right** contents

after change are stored in a region of utilization **right** contents. Incidentally, as utilization **right** contents, a plurality of kinds of contents exist for each utilization **right** content in one reproduction **right** with period limitation as a plurality kinds of reproduction **right** with period limitation exist by setting the period. Therefore, since it is difficult to manage utilization **right** contents only by a utilization **right** contents number, in the **right** contents changing **right**, utilization **right** contents are managed by a rule number attached for each of a plurality of contents for each of these utility **right** contents.

As shown in Figure 45J, as data of the repurchase **right**, information on an effective period of the repurchase **right** that indicates an effective period of a repurchase **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period until a date on which the period expires, or the like, an old rule number for retrieving utilization **right** contents before repurchase, and a new rule number for retrieving utilization **right** contents after repurchase, and maximum distribution generation information that indicates the maximum number of times contents can be repurchased are stored in a region of utilization **right** contents.

As shown in Figure 45K, as data of the additional purchase **right**, information on an effective period of the additional purchase **right** that indicates an effective period of an additional purchase **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period... ...maximum holding contents number indicating single contents already purchased among a plurality of single contents forming album contents are stored in a region of utilization **right** contents.

As shown in Figure 45L, as data of the management transfer **right**, information on an effective period of the management transfer **right** that indicates an effective period of a management transfer **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period until a date on which the period expires, or the like is stored in a region of utilization **right** contents.

Incidentally, as such utilization **right** contents, for example, when data of a game is divided into a plurality of contents, a contents purchase **right** for purchasing the contents in accordance with a predetermined order may be provided for. Further, as shown in Figure 45M, as data of the contents purchase **right**, information on an effective period of the contents purchase **right** that indicates an effective period of a contents purchase **right** by a date on which the period expires, or the number of days from a date to be a basis of starting an effective period until a date on which the period expires, or the like, an ID of contents already purchased, an old rule number for retrieving utilization **right** contents already purchased, and a new rule number for retrieving utilization **right** contents to be purchased anew are stored in a region of utilization **right** contents. In this way, a game program having a series of stories is made to be purchased, and contents (game) themselves can be upgraded.

Figure... ...data to be a basis when distribution is started until the period expires, or the like. The category of contents indicates whether the contents are **music** data, program data, video data, or the like, and the ID of contents is for identifying the single contents.

The ID of a content provider...and the processing is terminated.

Figure 53 illustrates operations when a settlement available apparatus in the user home network 5 transmits charge information to the **electronic** distribution service center 1. The settlement available apparatus in the user home network 5 retrieves an object apparatus that it should settle on behalf of... ...and sent (a signature is attached to the data then) . After finishing processing for all the apparatuses, the settlement available apparatus mutually authenticates with the **electronic** distribution service center 1, encrypts all the charge information with the shared temporary key, attaches signature data to these, and transmits them to the **electronic** distribution service center 1 together with a handling policy and price information, if necessary. Further, since an ID of a handling policy, an ID of price information and the like that are necessary for distribution of an amount are included in the charge information to be transmitted to the **electronic** service center 1 from the user home network 5, a handling policy or price information with large information amount is not necessarily transmitted. The user... ...encrypt them with the temporary key Ktemp)) and makes them invisible from outside. On the other hand, since, even if contents of charge information and **license** conditions information are seen, data cannot be illegally utilized, it is not always necessary to encrypt them with the temporary key Ktemp)), but damages to parties relating to receipt of an amount are generated if, for example, an amount of charge information is tampered or usage conditions of **license** conditions information is tampered to be loose. Therefore, tamper is prevented by attaching a signature to the charge information or the **license** conditions information. However, a signature may be attached if a content key Kco)) or a delivery key Kd)) is transmitted.

Then, a transmitting side generates...every actions including use, stoppage of purchase processing, state in which processing was conducted normally).

Figure 54 illustrates operations of profit distribution processing of the **electronic** distribution service center 1. The history data management section 15 maintains and manages charge information transmitted from the user management section 18, a handling policy, if necessary, and price information. The profit distribution section 16 calculates profit for each of the content provider 2, the service provider 3 and the **electronic** distribution service center 1 from the charge information, the handling policy, if necessary, and the price information transmitted from the history data management section 15... ...included in data in the charge information supplied from an apparatus in the user home network 5.

Figure 55 illustrates operations of processing in the **electronic** distribution service center 1 for transmitting utilization results of contents to JASRAC. The history data management section 15 transmits charge information indicating utilization results of...a flow chart illustrating processing of distribution and reproduction of contents of this system. In step S40, the content provider management section 12 of the **electronic** distribution service center 1 transmits an individual key Kl)) encrypted by a delivery key Kd)) and a public key certificate of the content provider 2... ...15) of the user home network 5, and registers the apparatus of the user home network 5 in the user

management section 18 of the **electronic** distribution service center 1. Details of this registration processing will be described later with reference to a flow chart of Figure 59. In step S42, the user management section 18 of the **electronic** service center 1, after mutually authenticating with the user home network 5 as described above with reference to Figure 52, transmits the delivery key Kd... ...flow chart of Figure 72.

Figure 57 is a flow chart illustrating details of processing, which corresponds to S40 of Figure 56, in which the **electronic** distribution service center 1 transmits an individual key Kl)), an individual key Ki)) encrypted by a delivery key Kd)) and a public key certificate to the content provider 2, and the content provider 2 receives these. In step S50, the mutual authentication section 17 of the **electronic** distribution service center 1 mutually authenticates with the mutual authentication section 39 of the content provider 2. Since the mutual authentication processing was described in... ...key Ki)), the individual key Ki)) encrypted by the delivery key Kd)) and the certificate transmitted from the content provider management section 12 of the **electronic** distribution service center 1. In step S52, the content provider 2 stores the received individual key Kl)) in the tamper resistant memory 40A, and stores... ...way, the content provider 2 receives an individual key Kl)), an individual key Kl)) encrypted by a delivery key Kd)) and a certificated from the **electronic** distribution service center 1. Similarly, in an example in which processing of the flow chart shown in Figure 56 is conducted, the service provider 3... ...from the individual key Ki)) of the content provider 2), an individual key Kl)) encrypted by a delivery key Kd)) and a certificate from the **electronic** distribution service center 1 with similar processing as that in Figure 57.

Further, the memory 40A is desirably a tamper resistant memory whose data is... ...Figure 58 is a flow chart illustrating processing in which the home server 51 registers settlement information in the user management section 18 of the **electronic** distribution service center 1. In step S60, the home server 51 mutually authenticates a public key certificate stored in the mass storage section 68 with the mutual authentication section 17 of the **electronic** distribution service center 1 in the mutual authentication module 95 of the encryption processing section 65. Since this authentication processing is similar to that described with reference to Figure 52, description is omitted here. A certificate that the home server 51 transmits to the user management section 18 of the **electronic** distribution service center 1 in step S60 includes data (a public key certificate of a user apparatus) shown in Figure 32.

In step S61, the...The data is encrypted in the encryption unit 112 using a temporary key Ktemp)), and is transmitted to the user management section 18 of the **electronic** distribution service center 1 via the communication section 61.

In step S63, the user management section 18 of the **electronic** distribution service center 1 takes out an ID of an apparatus from the received certificate, and retrieves through the user registration database shown in Figure 7 based on the ID of an apparatus. In step S64, the user management section 18 of the **electronic** distribution service center 1 decides whether or not registration of an apparatus having the received ID is possible, and if it is

decided that the... ...apparatus having the received ID is a new registration, the processing proceeds to step S66.

In step S66, the user management section 18 of the **electronic** distribution service center 1 issues a settlement ID anew, and at the same time, decrypts the settlement information encrypted by the temporary key, registers the... ...registration database. Since this registration information is described in Figure 8, its details are omitted.

In step S68, the user management section 18 of the **electronic** distribution service center 1 transmits the prepared registration information to the home server 51. In step S69, the upper controller 62 of the home server... ...63. The data is encrypted in the encryption unit 112 using a temporary key Ktemp)), and transmitted to the user management section 18 of the **electronic** distribution service center 1 via the communication section 61 together with the registration information already issued upon settlement registration.

In step S64, if it is... ...that registration of an apparatus having a received ID is indispensable, the processing proceeds to step S71, where the user management section 18 of the **electronic** distribution service center 1 prepares registration information of registration rejection, and the processing proceeds to step S68.

In step S65, if it is determined that the apparatus having the received ID is not a new registration, the processing proceeds to step S72, where the user management section 18 of the **electronic** distribution service center 1 decrypts the settlement information encrypted by the temporary key, and updates and registers it in the settlement information registration database by... ...it with the ID of the apparatus, and the processing proceeds to step S67.

In this way, the home server 51 is registered in the **electronic** distribution service center 1.

Figure 59 is a flow chart illustrating processing for registering an ID of an apparatus in registration information anew. Since mutual... ...step S82 is the same as step S64 of Figure 58, its description is omitted. In step S83, the user management section 18 of the **electronic** distribution service center 1 sets a registration item corresponding to an apparatus ID in the user registration database as "registration, " and registers the apparatus ID. In step S84, the user management section 18 of the **electronic** distribution service center 1 prepares registration information as shown in Figure 8 based on the user registration database. Since step S85 is the same as... ...that registration of an apparatus having a received ID is indispensable, the processing proceeds to step S87, where the user management section 18 of the **electronic** distribution service center 1 prepares registration information of registration rejection, and the processing proceeds to step S85.

In this way, the home server 51 is registered in the **electronic** distribution service center 1.

Figure 60 is a flow chart illustrating processing in additionally registering another apparatus via an already registered apparatus. Here, an example... ...processing is similar to the processing described in Figure 52, its description is omitted. In step S91, the home server 51 mutually authenticates with the **electronic** distribution service center 1. In step S92, the home server 51 transmits the registration information read out from the mass storage section 68 and the certificate of the fixed apparatus 52 obtain when mutually authenticating with the fixed apparatus 52 in step S90 to the **electronic** distribution service center 1. Since step S93 is the same as step S81 of Figure 59, its description is omitted. Since step S94 is the 18 of the **electronic** distribution service center 1 prepares registration information anew with information of the fixed apparatus 52 added in addition to the registration information received from the... ...that registration of an apparatus having a received ID is indispensable, the processing proceeds to step S99, where the user management section 18 of the **electronic** distribution service center 1 prepares registration information indicating that only the fixed apparatus 52 is rejected registration (therefore, the home server 51 stays registered), and the processing proceeds to step S97 (the fact that the home server 51 has succeeded in mutual authentication with the **electronic** distribution service center 1 means that the home server 51 is registrable.)

In this way, the fixed apparatus 52 is additionally registered in the **electronic** distribution service center 1 by the processing procedures indicated in Figure 60.

Timing for a registered apparatus to conduct update of a registration (update of...by the signature generation unit 114, and adds a signature. Then, the home server 51 transmits the encrypted charge information and its signature to the **electronic** distribution service center 1 together with a handling policy, price information and registration information stored in the mass storage section 68. Further, at this moment... ...be sent by a model. This is because, in some cases, the content provider 2 and the service provider 3 have transmitted them to the **electronic** distribution service center 1 in advance, or necessary information among the handling policy and the price information is included in the charge information.

Since step... ...step S103 is the same as step S82 of Figure 59, its description is omitted. In step S104, the user management section 18 of the **electronic** distribution service center 1 verifies a signature by the signature verification unit 115, decrypts received charge information by a temporary key Ktemp)) (if an **electronic** signature is attached to the received data, it is verified by the signature verification unit 115), and (if received) transmits the charge information to the... ...The history data management section 15 having received this maintains and manages the received data.

In step S105, the user management section 18 of the **electronic** distribution service center 1 verifies a registration item corresponding to an apparatus ID in the user registration database, and at the same time, updates data... ...Since step S106 is the same as step S84 of Figure 59, its description is omitted. In step S107, the user management section of the **electronic** distribution service center 1 encrypts a delivery key Kd)) supplied from the key server 14 by a temporary key Ktemp)), and transmits the delivery key... ...In step S109, the home server 51 inputs the received registration information in the encryption

processing section 65, where the home server 51 verifies an **electronic** signature included in the registration information by the signature verification unit 115, and at the same time, causes the unit to confirm if an apparatus... ...that registration of an apparatus having the received ID is impossible, the processing proceeds to step S111, where the user management section 18 of the **electronic** distribution service center 1 prepares registration information indicating that registration is rejected, and the processing proceeds to step S112. In step S112, which is different... ...a predetermined error processing is performed.

In this way, the home server 51 updates registration information, at the same time, transmits charge information to the **electronic** distribution service center 1, and receives supply of a delivery key Kd)) in return.

Figures 63 and 64 illustrate flow charts describing processing for settlement...charge information encrypted by the temporary key Ktemp)).

In step S124, the home server 51 mutually authenticates with the mutual authentication section 17 of the **electronic** distribution service center 1, and shares a temporary key Ktemp2)). In step S125, the home server 51 encrypts the charge information transmitted from the fixed... ...its signature, as well as the handling policy, the price information and the registration information, if necessary, to the user management section 18 of the **electronic** distribution service center 1.

In step S126, the user management section 18 of the **electronic** distribution service center 1 retrieves through the user registration database. In step S127, the user management section 18 decides whether or not the home server... ...and if it is decided that they are registered, the processing proceeds to step S128. In step S128, the user management section 18 of the **electronic** distribution service center 1 verifies a signature for the charge information encrypted by the temporary key Ktemp2)), and decrypts the charge information by the temporary... ...as the handling policy and the price information, if received, manages and stores the data.

In step S129, the user management section 18 of the **electronic** distribution service center 1 updates the user registration database (charge data receipt data and time, issued data and time of registration information, date and time of a delivery key, etc.). In step S130, the user management section 18 of the **electronic** distribution service center 1 prepares registration information (e.g., an example of Figure 8). In step S131, the user management section 18 of the **electronic** distribution service center 1 encrypts the delivery key Kd)) received from the key server 14 of the **electronic** distribution service center 1 by the temporary key Ktemp2)), and generates a signature for the delivery key Kd)) encrypted by the temporary key Ktemp2)). Then...the delivery key Kd)) encrypted by the temporary key Ktemp)), transmits them to the fixed apparatus 52 together with the registration information transmitted from the **electronic** distribution service center 1.

In step S133, the upper controller 72 of the fixed apparatus 52 overwrites and stores the received registration information in the... ...S137. Since the step S137 is the same as step

S130, its details are omitted. In step S138, the user management section 18 of the **electronic** distribution service center 1 transmits the registration information to the home server 51. In step S139, the home server 51 transmits the registration information to...
...3, which corresponds to step S43 of Figure 56, will be described with reference to a flow chart of Figure 65. In step S140, the **electronic** watermark adding section 32 of the content provider 2 inserts predetermined data indicating the content provider 2, for example, a content provider ID, in the contents read out from the content server 31 in the form of an **electronic** watermark, and supplies it to the compression section 33. In step S141, the compression section 33of the content provider 2 compresses the contents in which the **electronic** watermark is inserted by a predetermined method such as ATRAC, and supplies to the content encryption section 34. In step S142, the content key generation section 35 generates a key to be **used** as a **content** key Kco)), and supplies it to the content encryption section 34 and the content key encryption section 36. In step S143, the content encryption section 34 of the content provider 2 encrypts the compressed contents in which the **electronic** watermark is inserted by a predetermined method such as DES using the content key Kco)).

In step S144, the content key encryption section 36 encrypts the content key Kco)) with the individual key K1)) supplied from the **electronic** distribution service center 1 by the processing of step S40 of Figure 56 by a predetermined method such as DES. In step S145, the handling...51. Further, the input processing may be performed upon starting the purchase processing. The encryption processing section 65 having received this generates charge information and **license** conditions information from the handling policy inputted in step S167 and the price information inputted in step S169. Since the charge was described in Figure 42, its details are omitted. Since the **license** conditions information was described in Figure 41, its details are omitted.

In step S171, the control section 91 of the encryption processing section 65 stores...
...information generated in step S170 in the storage module 92. In step S172, the control section 91 of the encryption processing section 65 transmits the **license** conditions information generated in step S170 to the external memory control section 97 of the encryption processing section 65. After checking tamper of the external memory 67, the external memory control section 97 having received the **license** conditions information writes the **license** conditions information in the external memory 67. Tamper check in writing the **license** conditions information will be described latter with reference to Figure 69. In step S173, the control section 91 of the encryption processing section 65 decrypts...external memory 67. At this moment, data other than the data that is planned to be read out (e.g., a content key 1 and **license** conditions information 1) is destroyed after used for the hash value calculation. In step S182, the hash value calculated in step S181 and a hash...memory control section 97 of the encryption processing section 65, and causes the external memory control section 97 to retrieve a content key Kco)) and **license** conditions information corresponding to the content ID. At this moment, the control section 91 confirms that the **license** conditions information is a **right** that can be reproduced. In step S202, the external memory control section 97 of the encryption processing section 65 calculates a hash value of a data block including the content key Kco)) and the **license** conditions information, and transmits the hash value to the control

section 91 of the encryption processing section 65. In step S203, the control section 91...
...if the hash values coincide, the processing proceeds to step S204.

In step S204, the control section 91 of the encryption processing section 65 updates
license conditions information, if necessary. For example, if a utilization **right** in the
license conditions information is a commutation ticket, the control section 91 performs
processing such as for subtracting the number of times. Therefore, in case of a buy only
right or the like that does not need to be updated, the processing jumps to step S208 (not
shown) . In step S205, the external memory control section 97 rewrites the updated
license conditions information transmitted from the control section 91 to the external
memory 67 and updates it. In step S206, the external memory control section 97...
...module 104 of the extension section 66 extends the contents with a predetermined
method, for example, such a method as ATRAC. In step S215, the **electronic** watermark
addition module 105 inserts the data instructed by the encryption processing section 65 in
the contents in the form of a watermark (the data... ...to the extension section from the
encryption processing section is not limited to the content key Kco)), but includes
reproduction conditions (an analogue output, a **digital** output, an output with copy control
signal (SCMS)), an apparatus ID that purchased the content utilization **right** and the like.
Data to be inserted is an ID of an apparatus that purchased the content utilization **right**
(i.e., an apparatus ID in the **license** conditions information) or the like. In step S216, the
extension section 66 reproduces **music** via a speaker (not shown).

In this way, the home server 51 reproduces contents.

Figure 74 is a flow chart illustrating details of processing in which the home server 51
purchases a content utilization **right** on behalf of the fixed apparatus 52. In step S220, the
home server 51 and the fixed apparatus 52 mutually authenticates. Since the mutual
authentication... ...signature verification unit 115 of the encryption/decryption module 96
to verify a signature attached to the registration information by a public key of the
electronic distribution service center 1 supplied form the storage module 92 of the
encryption processing section 65. After successful verification of the signature, the
control section... ...signature generation unit 114 of the encryption/decryption module 96
with respect to the content key Kco)) encrypted by the temporary key Ktemp)) and the
license conditions information generated in step S226, and transmits them to the upper
controller 62. The upper controller 62 of the homes server 51 having received the content
key Kco)) encrypted by the temporary key Ktemp)), the **license** conditions information
and their signatures reads out the contents (including a signature; hereinafter the same)
encrypted by the content key Kco)) from the mass storage section 68, and transmits the
content key Kco)) encrypted by the temporary key Ktemp)), the **license** conditions
information, their signatures and the contents encrypted by the content key Kco)) to the
fixed apparatus 52.

In step S230, the fixed apparatus 52 having received the content key Kco)) encrypted by
the temporary key Ktemp)), the **license** conditions information, their signatures and the
contents encrypted by the content key Kco)) outputs the contents encrypted by the
contents key Kco)) to the record... ...step S232, the encryption processing section 73 of

the fixed apparatus 52 transmits the content key Kco)) encrypted by the save key Ksave2)) and the **license** conditions information received in step S230 to the external memory control section of the encryption processing section 73, and causes the external memory 79 to... ...writes data in the external memory was described in Figure 69, details are omitted.

In this way, the home sever 51 purchases a content utilization **right**, charge information is stored in the home server 51 side, and a utilization **right** is transferred to the fixed apparatus 52.

Figure 75 is a flow chart illustrating processing for changing a purchased content utilization **right** to another utilization form to purchase it. Since steps S240 to S245 are similar to the processing described in Figure 67, its description is omitted...encryption processing section 65 of the home server 51 causes the external memory control section 97 of the encryption processing section 65 to read out **license** conditions information of contents whose utilization **right** is changed. Since reading out of data from the external memory 67 was described with reference to Figure 68, its details are omitted. If the **license** conditions information is correctly read out in step S246, the processing proceeds to step S247.

In step S247, the upper controller 62 of the home server 51 displays information of content whose utilization **right** contents can be changed (e.g., a utilization form or a price whose utilization **right** contents can be changed) using the display means 64, and a user selects utilization **right** contents update conditions using the inputting means 63. The signal inputted from the inputting means 63 is transmitted to the upper controller 62 of the home server 51, and the upper controller 62 generates a utilization **right** content change command based on the signal and inputs the utilization **right** contents change command in the encryption processing section 65 of the home server 51. The encryption processing section 65 having received this generates charge information and new **license** conditions information from the handling policy received in step S243, the price information received in step S245 and the **license** conditions information read out in step S247.

Since step S248 is similar to step S171 of Figure 67, its detailed description is omitted. In step S249, the control section 91 of the encryption processing section 65 outputs the **license** conditions information generated in step S247 to the external memory control section 97 of the encryption processing section 65. The external memory control section 97 overwrites the received **license** conditions information in the external memory 67 and updates it. Since the method of rewriting (updating) method to the external memory 67 of the external memory control section 97 was described in Figure 70, its details are omitted.

In step S246, if **license** conditions information corresponding to the content ID attached to the **right** contents change command was not found in the external memory 67, or if tamper was found in a storage block of the external memory in which the **license**

conditions information is stored (which has been described with reference to Figure 68), the processing proceeds to step S251, and predetermined error processing is performed.

In this way, the home server 51 can purchase a new **right** using an already purchased **right** (described in the **license** conditions information), a handling policy and price information, and change utilization **right** contents.

Figures 76 and 77 illustrate concrete examples of a rule portion of a handling policy and price information. In Figure 76, the handling policy is composed of a rule number attached to each utilization **right** as a serial number, a utilization contents number indicating utilization **right** contents, its parameter, a minimum sales price, and a profit ratio of a content provider, in which, for example, five rules are written. Since a rule 1 has a utilization **right** contents number 1 as a **right** item, it is seen from Figure 44 that the **right** is a **right** without a reproduction **right**, time and number of times limitations. In addition, it is seen that there is no specific description in the item of a parameter. The minimum sales price is (Yen)350, and a share of the content provider 2 is 30% of the price. Since a rule 2 has a utilization **right** contents number 2 as the **right** item, it is seen from Figure 44 that the **right** is a **right** with a reproduction **right** and time limitation and without number of times limitation. In addition, it is seen from the item of a parameter that a utilization possible period... ...sales price is (Yen)100, and the share of the content provider 2 is 30% of the price. Since a rule 3 has a utilization **right** contents number 6 as the **right** item, it is seen from Figure 44 that the **right** is a **right** without a reproduction **right** (without a copy control signal), without time limitation and with number of times limitation. In addition, it is seen from the item of a parameter... ...sales price is (Yen)30, and the share of the content provider 2 is 30% of the price.

Since a rule 4 has a utilization **right** contents number 13 as the **right** item, it is seen from Figure 44 that the **right** is utilization contents change. It is seen from the item of a parameter that a changeable rule number from #2 (with a reproduction **right**, with time limitation and without number of times limitation) to #1 (without a reproduction **right**, time and number of times limitation) . The minimum price is (Yen)200, and the share of the content provider 2 is 20% of the price. The minimum sales price is presented lower than that of the rule 1 because it is considered that an already purchased **right** it traded in and repurchased, and the share of the content provider 2 is presented lower than that of the rules 1 in order to increase the share of the **electronic** distribution service center 1 that performs actual work (since the content provider 2 has no work at the time of **right** contents change).

Since a rule 5 has a utilization **right** contents number 14 as the **right** item, it is seen from Figure 44 that the **right** is redistribution. It is seen from the item of a parameter that redistribution possible conditions is that an apparatus having the rule number #1 (without a reproduction **right**, time and number of times limitation) purchases and redistribute the rules number #1 (without a reproduction **right**, time and number of times limitation) . The minimum sales price is (Yen)250, and the share of the content provider 2 is 20% of the price. The minimum sales price is lower than that of the rule 1 because it is considered that an apparatus having an already purchased **right** repurchases identical

contents, and the share of the content provider 2 is presented lower than that of the rule 1 in order to increase the share of the **electronic** distribution service center 1 that performs actual work (since the content provider 2 does not have work at the time of redistribution).

In Figure 77, the price information is composes of a rule number attached to each utilization **right** as a serial number, a parameter and price information. Five rules are also described in this price information. A rule 1 is price information corresponding...
...Therefore, out of (Yen)500 paid by a user, the content provider 2 takes (Yen)150, the service provider 3 takes (Yen)150, and the **electronic** distribution service center 1 takes (Yen)200. Since rules 2 to 5 are similar, their details are omitted.

Further, in rules 4 and 5, the... ...2 is fewer than that of the rule 1 because a user apparatus performs distribution work on behalf of the service provider 2, and the **electronic** distribution service center 1 performs collection of prices.

In addition, although the rule numbers are serial numbers from #1 to #5 in this example, this... ...rule number, and arranges ones extracted from the numbers, the rule numbers are not generally serial numbers.

Figure 78 illustrates a specific example when the **right** contents change described in Figure 75 is performed. The handling policy is composed of a rule number attached to each utilization **right** as a serial number, a utilization contents number indicating utilization **right** contents, it parameter, a minimum sales price, and a profit ratio of a content provider, the price information is composes of a rule number attached to each utilization **right** as a serial number, a parameter and price information, and the **license** conditions information is composed of a rule number attached to each utilization **right** as a serial number, a utilization **right** contents number indicating utilization **right** contents, and its parameter. The home server 51 has already purchased a **right** with a reproduction **right** with the rule number #2 and time limitation, and the rule number #2 is described in the **license** conditions information indicating **right** contents, which indicates that remaining utilization possible time is thirty minutes, and accumulated two hours of purchase has been performed so far. If it is tried to change the **right** from with time limitation to without time limitation now, it is seen from a rule 3 of the handling policy, a rule 3 of the price information and the **license** conditions information that the **right** can be changed to without a reproduction **right**, time and number of times limitation with (Yen)200, and the **license** conditions information changes to without a reproduction **right**, time and number of times limitation of the rule number #1 and the utilization **right** contents number (a parameter in case of the utilization **right** contents number #1 will be described later. In addition, in this example, changing the **right** contents once after buying a **right** with time limitation is cheaper than directly buying a **right** without a reproduction **right**, time and number of times limitation. Thus, it is better to put a discount considering accumulated utilization time.

Figure 79 is a flow chart illustrating details of processing in which the home server 51 purchases a content utilization **right** for the fixed apparatus 52 and redistributes the

utilization **right**. Since steps S260 to S264 are similar to steps S220 to S225 of Figure 74, their detailed description is omitted. In step S265, the encryption... ...the home server 51 causes the external memory control section 97 of the encryption processing section 65 to read out from the external memory 67 **license** conditions information and the content key Kco)) encrypted by the save key Ksave)) corresponding to contents that is tried to be redistributed. Since a method... ...command in the encryption processing section 65 of the home server 51. The encryption processing section 65 having received this generates charge information and new **license** conditions information from the handling policy and the price information received in step S264, and the **license** conditions information read out in step S265.

Since step S267 is similar to step S171 of Figure 67, its detailed description is omitted. In step...unit 114 of the encryption/decryption module 96 generates signatures corresponding to the content key Kco)) encrypted by the temporary key Ktemp)) and the new **license** conditions information generated in step S266, and returns it to the control section 91 of the encryption processing section 65.

Since processing of steps S269... ...S229 to S232 of Figure 74, its details are omitted.

In this way, the home server 51 can perform redistribution of contents by creating new **license** conditions information from a utilization **right** (**license** conditions information) it owns and a handling policy, price information, and transmitting the information to the fixed apparatus 52 together with the content key Kco)) and contents it owns.

Figure 80 is a flow chart illustrating details of processing in which the home server 51 transmits **license** conditions information and content key Kco)) to the fixed apparatus 52 and the fixed apparatus 52 purchases a content utilization **right**. In step S280, the encryption processing section 73 of the fixed apparatus 52 decides whether or not a total of charges of charge information stored... ...section 91 of the encryption processing section 65 generates signatures with respect to the content key Kco)) encrypted by the temporary key Ktemp)) and the **license** conditions information read out in step S284 using the signature generation unit 114 of the encryption/decryption module 96, and transmits them to the upper controller 62. The upper controller 62 of the home server 51 having received the content key Kco)) encrypted by the temporary key Ktemp)) and the **license** conditions information and their signatures reads out the contents encrypted by the content key Kco)), the handling policy and its signature, if necessary, and the price information and its signature from the mass storage section 68, and transmits the content key Kco)) encrypted by the temporary key Ktemp)) and the **license** conditions information, the contents encrypted by the content key Kco)), the handling policy and its signature, and the price information and its signature to the... ...command in the encryption processing section 73 of the fixed apparatus 52. The encryption processing section 73 having received this generates charge information and new **license** conditions information from the handling policy, the price information and the **license** conditions information received in step S286.

In step S290, the encryption processing section 73 of the fixed apparatus 52 stores the charge information generated in... ...storage module (not shown) of the encryption processing section 73.

In step S292, the encryption processing section 73 of the fixed apparatus 52 transmits the **license** conditions information generated in step S289 and the content key Kco)) encrypted by the save key Ksave2)) generated in step S291 to an external memory control section (not shown) of the encryption processing section 73. The external memory control section having received the **license** conditions information and the content key Kco)) encrypted by the save key Ksave2)) writes the **license** conditions information and the content ...with reference to Figure 69, its details are omitted.

In this way, the fixed apparatus 52 can receive redistribution of contents by receiving a utilization **right** (**license** conditions information) owned by the home server 51, a handling policy, price information, a content key Kco)), and contents from the home server 51, and creating new **license** conditions information in the fixed apparatus 52.

Figure 81 illustrates a managed transfer **right**. Managed transfer means an operation capable of transferring a reproduction **right** from an apparatus 1 to an apparatus 2, which is the same as normal transfer in that the **right** is transferred from the apparatus 1 to the apparatus 2, but is different from normal transfer in that the apparatus 2 cannot retransfer the received reproduction **right** (the apparatus 1 after transferring a reproduction **right** cannot retransfer the reproduction **right** as in the normal transfer) . The apparatus 2 having received the reproduction **right** by the managed transfer can return the reproduction **right** to the apparatus 1, and after returning the reproduction **right**, the apparatus 1 can transfer the reproduction **right** again and the apparatus 2 cannot continue to transfer the reproduction **right**. In order to realize these, a purchaser of the managed transfer **right** and a current holder of the managed transfer **right** are managed in the **license** conditions information (here, it is assumed that the managed transfer can only be performed if the utilization content number #1 is held, but this can be extended to the utilization **right** content number #2).

In Figure 81, since the rule 1 of the handling policy was described in Figure 78, its details are omitted. Since a **right** item of the rule 2 is the utilization **right** content number 16, it is seen from Figure 44 that the **right** is the managed transfer **right**. In addition, it is seen that there is no specific description in the item of a parameter. The minimum sales price is (Yen)100, and... ...of a handling policy, and indicates that the price is (Yen)100 and the share of the service provider 3 is 0% when the utilization **right** content number #16 is purchased. Therefore, out of (Yen)100 paid by a user, the content provider 2 takes (Yen)50, the service provider 3 takes (Yen)0, and the **electronic** distribution service center 1 takes (Yen)50.

In Figure 81, the user first purchases the rule number #1 (without a reproduction **right**, time and number of times limitation). However, the user does not have the managed transfer **right** then (the state of a in Figure 81). Then, the user purchases the managed transfer **right** (since these operations happens in an instance, it looks as if the user

purchased all at a time). Concerning the rule number of the **license** conditions, an ID of an encryption processing section indicating a purchase (hereinafter referred to as a purchaser) is ID1 (e.g., an ID of the home server 51), and an ID of an encryption processing section holding the reproduction **right** (hereinafter referred to as a holder) is ID2 (the state of b in Figure 81). If this is transferred to the fixed apparatus 52 by performing the managed transfer, in the rule section of the **license** conditions information held by the home server 51, the purchase is still ID1, but the holder is changed to ID2. In addition, in the rule section of the **license** conditions information held by the fixed apparatus 52 having received the reproduction **right** by the managed transfer, the purchase is ID1 and the holder is ID2, which is the same as the **license** conditions information of the home server 51.

Figure 82 is a flow chart illustrating details of the transfer processing of the managed transfer **right**. In Figure 82, since step S300 is similar to step S220 of Figure 74, its details are omitted. In addition, since step S301 is similar... ...its details are omitted. In step S303, the encryption processing section 65 of the home server 51 inspects the rule section of the read out **license** conditions information, and decides if the use **right** is without the reproduction **right**, time and number of times limitation and with the managed transfer **right**. If it is decided that there is the managed transfer **right**, the processing proceeds to step S304.

In step S304, the control section 91 of the encryption processing section 65 decides if both the purchaser and the holder of the managed transfer **right** are the ID of the home server 51. If it is decided that both the purchase and the holder of the managed transfer **right** is the ID of the home server 51, the processing proceeds to step S305. In step S305, the control section 91 of the encryption processing section 65 rewrites the holder of the managed transfer **right** of the **license** conditions information to the ID of the fixed apparatus 52. In step S306, the control section 91 of the encryption processing section 65 outputs the **license** conditions information rewritten in step S305 to the external memory control section 97 of the encryption processing section 65. The external memory control section 97 of the encryption processing section 65 having received the **license** conditions information overwrites the **license** conditions information on the external memory ...are omitted. Since steps S307 to S311 are similar to steps S268 to S272 of Figure 79, their details are omitted.

If the managed transfer **right** was not included in the **license** conditions information in step S303, or if the purchase or the holder of the managed transfer **right** was not the home server 51 in step S304, the processing is terminated.

In this way, the **right** for reproducing contents from the home server 51 to the fixed apparatus 52 can be transferred.

Figure 83 is a flow chart illustrating processing for returning the managed transfer **right** from the fixed apparatus 52 currently holding the managed transfer **right** to the home server 51 that is the purchaser of the managed transfer **right**. In Figure 83, since step S320 is similar to step S220 of Figure 74, its details are omitted. Since step S321 is

similar to step... ...Figure 82, its details are omitted, but it is decided that both the home server 51 and the fixed apparatus 52 have the managed transfer **right**. If it is decided that there is the managed transfer **right**, the processing proceeds to step S324.

In step S324, the encryption processing section 65 of the home server 51 decides if the purchaser of the managed transfer **right** is the ID of the homes server 51 and the holder is the ID of the fixed apparatus 52. If it is decided that the purchaser of the managed transfer **right** is the ID of the home server 51 and the holder is the ID of the fixed apparatus 52, the processing proceeds to step S325. Similarly, the encryption processing section 73 of the fixed apparatus 52 decides if the purchaser of the managed transfer **right** is the ID of the home server 51 and the holder is the ID of the fixed apparatus 52. If it is decided that the purchaser of the managed transfer **right** is the ID of the home server 51 and the holder is the ID of the fixed apparatus 52, the processing proceeds to step S325... ...the encryption processing section 73 to delete the content key Kco)) encrypted by the save key Ksave2)) stored in the external memory 79 and the **license** conditions information. Since the deletion method of data of the external memory 79 was described in Figure 71, its details are omitted.

In step S327, the control section 91 of the encryption processing section 65 generates **license** conditions information in which the holder of the managed transfer **right** of the **license** conditions information to the ID of the home server 51. In step S328, the control section 91 of the encryption processing section 65 outputs the **license** conditions information generated in step S327 to the external memory control section 97 of the encryption processing section 65. The external memory control section 97 of the encryption processing section 65 having received the **license** conditions information overwrites and stores the **license** conditions information in the external memory 67. Since the method for rewriting and storing in the external memory 67 was described in Figure 70, its... ...other apparatus was not registered in the homes server 51 or the fixed apparatus 52 in step S321, or if the content key or the **license** conditions information with respect to predetermined contents was not found in the external memory or the memory block including these was tampered in the home server 51 or the fixed apparatus 52 in step S322, the processing proceeds to step S329 and error processing is performed.

If the managed transfer **right** did not exist in the **license** conditions information in the home server 51 or the fixed apparatus 52 in step S323, or if the purchase was the home server 51 and... ...the fixed apparatus 52 in the home server 51 or the fixed apparatus 52 in step S324, the processing is terminated.

In this way, a **right** for reproducing contents can be returned from the fixed apparatus 52 to the home server 51.

Further, although contents and the content key Kco)) or... ...as described above with reference to Figure 9. In addition, the content provider 2 receives an individual key peculiar to a content provider from the **electronic** distribution service center 1 and an individual key encrypted by a delivery key, and encrypts the content key by the individual key. Thus, ...the service provider 3.

The user home network 5 decrypts the individual key peculiar to a content provider using the delivery key received from the **electronic** distribution service center 1. Thus, the user home network 5 can decrypts the content key that is encrypted by the individual key peculiar to a... ...or the like of the content key Kco)) are described (e.g., a handling policy generation section 206 of Figure 84), means for generating a **digital** signature with respect to various kinds of data (e.g., a signature generation section 207 of Figure 84), means for verifying signature data generated with... ...for receiving a reproduction command from an apparatus holding contents (e.g., the homes server 51) by an apparatus that does not hold a reproduction **right** of contents (e.g., the fixed apparatus 52) and reproducing the contents will be described.

Figure 86 shows remote reproduction processing procedures, and first, in... ...external memory control section 97 of the encryption processing section 65 to read out a content key Kco)) encrypted by a save key Ksave)) and **license** conditions information corresponding to the contents to be remotely reproduced from the ...ATRAC. In step S416, the upper controller 72 inserts data instructed by the encryption processing section 73 in the contents in the form of an **electronic** watermark. Incidentally, the data handed from the encryption processing section 73 to the extension section 74 is not limited to the content key Kco)) and the reproduction command, but includes reproduction conditions (an analog output, a **digital** output, an output with copy control signal (SCMS)), an ID of an apparatus that has purchased a content utilization **right**, or the like. The data to be inserted is the ID of the apparatus that has purchased the content utilization **right**, i.e., an ID of an apparatus in the **license** conditions information. In step S417, the extension section 74 reproduces **music** via a speaker (not shown).

In the above-described configuration, since the home server 51 transmits the contents and the reproduction command of the contents as well as the content key Kco)) to the fixed apparatus 52, the fixed apparatus 52 that does not hold the reproduction **right** of the contents can reproduce the contents using the reproduction command and the content key Kco)). Therefore, according to the above-described configuration, the contents can be reproduced in a plurality of apparatuses (a fixed apparatus, etc) connected to an apparatus holding the contents (an apparatus having the reproduction **right** of the contents).

(4) Reservation purchase processing

Reservation purchase processing for performing a purchase reservation of contents by performing key conversion of the contents in...a service provider corresponding to step S168, processing for signature verification of price information corresponding to step S169, and save processing of charge information and **license** conditions information corresponding to steps S170 through S172 may not be performed.

Incidentally, in the case of the reservation purchase processing of Figure 87, although the home server 51 did not prepare **license** conditions information, the home server 51 may prepare **license** conditions information and set its utilization **right** content number (i.e., a

right item) in a state without a **right** such as an initial value (e.g., #0 that does not exist), or the like.

In this way, in the reservation purchase processing, by saving...purchase command in the encryption processing section 65 of the home server 51. The encryption processing section 65 having received this generates charge information and **license** conditions information from the handling policy inputted in step S475 and the price information inputted in step S477. Since the charge information is as descried in Figure 42, its details are omitted. In addition, since the **license** conditions information is as described in Figure 41, its details are omitted.

In step S479, the control section 91 of the encryption processing section 65... ...generated in step S478 in the storage module 92. Then, in step S480, the control section 91 of the encryption processing section 65 transmits the **license** conditions information generated in step S478 to the external memory control section 97 of the encryption processing section 65. After checking tamper of the external memory 67, the external memory control section 97 having received the **license** conditions information writes the **license** conditions information in the external memory 67. Since the tamper check in writing is as described in Figure 69, its detailed description is omitted. (Further, if **license** conditions information without a **right** is already written, the **license** conditions information is rewritten and updated by the rewriting processing described in Figure 70.)

Incidentally, if it is decided in step 472 that the home... ...storing the charge information of the contents that a user selected to purchase in the storage module 92 and, at the same time, storing the **license** conditions information in the external memory 67. In the purchase processing, the signature verification of the content key Kco)) (step S454) and the signature verification...the control section 91 of the encryption processing section 65 generates signatures for the content key Kco)) encrypted by the temporary key Ktemp)) and the **license** conditions information generated in step S509 using the signature generation unit 114 of the encryption/decryption module 96, and transmits them to the upper controller 62. The upper controller 62 of the home server 51 having received the content key Kco)) encrypted by the temporary Key Ktemp)), the **license** conditions information and their signatures reads out the contents encrypted by the content key Kco)) from the mass storage section 68, and transmits the content key Kco)) encrypted by the temporary key Ktemp)), the **license** conditions information, their signatures and the contents encrypted by the content key Kco)) to the apparatus external to a group.

In step S513, the apparatus external to a group having received the content key Kco)) encrypted by the temporary key Ktemp)), the **license** conditions information, their signatures and the contents encrypted by the content key Kco)) outputs the contents encrypted by the content key Kco)) to the record... ...the encryption processing section 73 of the apparatus external to a group transmits the content key Kco)) encrypted by the save key Ksave2)) and the **license** conditions information received in step S513 to the external memory control section of the encryption processing section 73, and causes the external memory 79 to **right**, charge information is saved in the home server 51 side, and a utilization **right** is transferred to the apparatus external to a group. Thus, the home server

51 makes payment for the content utilization **right** transferred to the apparatus external to a group.

Figure 90 shows processing procedures in which the home server 51 passes contents to the apparatus external... ...the signal and inputs the purchase command in the encryption processing section 73. The encryption processing section 73 having received this generates charge information and **license** conditions information from the handling policy and the price information inputted in step S560. Since the charge information was described in Figure 42, its details are omitted. Since the **license** conditions information was described in Figure 41, its details are omitted.

In step S562, the encryption processing section 73 saves the charge information generated in... ...in the external memory 79 from the encryption processing section 73.

In this way, since the home server 51 transfers the already purchased content utilization **right** to the apparatus external to a group and the apparatus external to a group saves the charge information, the apparatus external to a group makes payment for the content utilization **right** transferred from the home server 51.

In the above-described configuration, by exchanging the registration information ...described in a handling policy or price information, and operations are performed in accordance with it.

(6) Data format of various kinds of data

The **electronic** distribution service center 1 adds an ID of the content provider 2 in an individual key Ki)) for each content provider 2, encrypts the entirety... ...to a corresponding content provider 2 as the encrypted individual key Ki)).

The content provider 2 stores the encrypted individual key Ki)) given by the **electronic** distribution service center 1 in this way in key data for single contents as it is, and delivers it to an apparatus in the user home network 5 via the service provider 3. Then, in the **electronic music** distribution system 10, the deliver key Kd)) for decrypting the encrypted individual key Ki)) included in the key data is held only by the apparatus... ...tampered during delivery and illegal contents are supplied, or a signature of a handling policy of the like is tampered during delivery.

Thus, in the **electronic music** distribution system 10, for example, purchase processing of illegal contents or generation of charge information for distributing profit illegally to a third party based on an illegal handling policy can be substantially certainly prevented, thereby preventing content data to be illegally utilized.

Incidentally, in such an **electronic music** distribution system 10, an ID of the service provider 3 may be encrypted and delivered in the same manner as an ID of the content... ...to illegally obtain profit, this can be easily and certainly prevented.

In addition, Figure 91 shows generation management by transfer processing of a managed transfer **right**. As described above with reference to Figures 33 and 34, how many generations of reproduction **rights** can be transferred at the most is stored in a handling policy as generation management information. Therefore, when the handling policy is given to a... ...contents to which the handling policy is attached according to the detected maximum number of times contents can be repurchased, the encryption processing section prepares **license** conditions information based on the handling policy, stores the ID of the encryption processing section in the **license** conditions information, and at the same time, stores a number of times found by deducting one from the maximum number of times contents can be... ...in the charge information.

Then, when the contents to which purchase processing was applied can be redistributed by the generation management information included in the **license** conditions information, a first apparatus redelivers the contents from the first apparatus to a second apparatus in the user home network 5 together with the **license** conditions information, if necessary. In the second apparatus, when executing purchase processing to the redelivered contents, the encryption processing section inside the second apparatus prepares the **license** conditions information attached to the contents again, stores the ID of the encryption processing section in the **license** conditions information prepared again, and at the same time, stores a number of times found by deducting one from the remaining number of times content in the **license** conditions information has been repurchased for the maximum number of times the purchase processing is possible set in advance, the second apparatus determines that redelivery is impossible and does not redeliver the contents.

Thus, in the **electronic music** distribution system 10, by providing for the maximum number of times contents can be repurchased in the handling policy in advance by the generation management information as described above, and managing a remaining number of times the contents can be repurchased in the **license** conditions information for each purchase processing of the contents, illegal repurchase can be prevented.

In addition, in the **electronic music** distribution system 10, by accumulating and storing an ID of a supplier of the contents by charge information upon repurchasing the contents, a supply route... ...information, if necessary, and, when illegal contents flows into the system, a supplier of the illegal contents can be retrieved and eliminated.

Incidentally, in the **electronic music** distribution system 10, since an apparatus in the user home network 5 provides the contents on behalf of the content provider 2 or the service provider 3 upon repurchasing the contents, for example, in the **electronic** distribution service center 1, profits can be returned to the apparatus by adding a discount point that can be used upon purchasing contents to a... ...a supplier of repurchase of the contents based on an ID of the supplier included in the charge information.

In above-described configuration, in the **electronic music** distribution system 10, in the case in which contents is provided to an apparatus in the user home network 5 via from the content provider... ...contents and the album contents as a content provider secure container.

Here, the content provider 2 then uses the individual Key Ki)) supplied from the **electronic** distribution service center 1 as an individual key Ki)) encrypted by the delivery key Kd)), whereas the **electronic** distribution service center 1 adds an ID of the content provider 2 to the individual key Ki)) and encrypts the entirety of these using the... ...Kd)). Then, the delivery key Kd)) used for this encryption is held only by an apparatus in the user home network 5 other than the **electronic** distribution service center 1.

Therefore, in the **electronic music** distribution system 10, the individual key Ki)) encrypted by the delivery key Kd)) can be provided from the content provider 2 to an apparatus in... ...as well as the handling policies of the single contents and the album contents can be easily and certainly detected.

As a result, in the **electronic music** distribution system 10, provision of illegal contents to a user or generation of charge information for a third party to illegally obtain profit using a handling policy can be prevented, thus, illegal utilization of contents by a third party can be prevented.

In addition, in the **electronic music** distribution system 10, a maximum number of times contents can be repurchased is stored in a handling policy provided from the content provider 2, and at the same time, a remaining number of times contents can be repurchased is stored in the **license** conditions information in the apparatus each time the contents are repurchased between apparatuses in the user home network 5.

Therefore, in the **electronic music** distribution system 10, an apparatus in the user home network 5 can manage a remaining number of times contents canbe repurchased by the **license** conditions information, thus, illegal repurchase exceeding the maximum number of times contents can be repurchased can be prevented.

According to the above-described configuration, by... ...the content provider 2 attached to the contents, whether or not the contents can be legally utilized can be easily and certainly determined, thus, an **electronic music** distribution system that can prevent contents from illegally utilized.

In addition, by storing a ...policy provided form the content provider 2, and at the same time, storing a remaining number of times the contents can be repurchased in the **license** conditions information in the apparatus to manage the number of times the contents can be repurchased, illegal repurchase exceeding the maximum number of times the contents can be repurchased can be prevented.

(7) Configuration of a record reproduction apparatus

In the **electronic music** distribution system 10, a record reproduction apparatus 250 shown in Figure 92 is provided as an apparatus in the user home network 5. In the record reproduction apparatus 250, an **electronic** distribution only recording medium 251 that is a data storage apparatus is detachably provided.

The record reproduction apparatus 250 can record contents electronically distributed from the service provider 3 via the network 4 in the **electronic** distribution only recording medium 251 and reproduce the contents from the **electronic** distribution only recording medium 251.

Actually, the record reproduction apparatus 250 is composed of a communication section 260 that is receiving means, an upper controller... ...263 that is content decrypting means, inputting means 264, displaying means 265, and a mass storage section 266. The communication section 260 communicates with the **electronic** distribution service center 1, and at the same time, communicates with the service provider 3 via the network 4.

The upper controller 261 once hold... ...service provider secure container received by the communication section 260 in the mass storage section 266 by controlling the record reproduction apparatus 250 and the **electronic** distribution only recording medium 251 based on an operation instruction inputted via the inputting means 264 at the time of purchase processing.

Then, the upper controller 261 causes the **electronic** distribution only recording medium 251 to execute purchase processing, thereby reads out contents encrypted by a corresponding content key Kco)), a content key Kco)) encrypted... ...by the delivery key Kd)) by a delivery key Kd)) read out from the storage module 311 of the encryption processing section 301 in the **electronic** distribution only recording medium 251, decrypts the content key Kco)) encrypted by the individual key Ki)) by the decrypted individual key Kl)), encrypts the obtained... ...and records the contents encrypted by the read out content key Kco)) and the content key Kco)) encrypted by the save key Ksave)) in the **electronic** distribution only recording medium 251.

In addition, the upper controller 261 reads out a content key Kco)) encrypted by a temporary key Ktemp1)) (shared by the encryption processing section 262 and the encryption processing section 301 by mutual authentication) from the **electronic** distribution only recording medium 251, and supplies a content key Kco)) encrypted by a temporary key Ktemp2)) (shared by the encryption processing section 262 and... ...263 to decrypt the contents encrypted by the content key Kco)) using the content key Kco)) by controlling the record reproduction apparatus 250 and the **electronic** distribution only recording medium 251 based on an operation instruction inputted via the inputting means 264 at the time of reproduction processing.

Incidentally, since the... ...the homes server 51, their descriptions are omitted.

In addition, the mutual authentication module 274 executes mutual authentication with the extension section 263 and the **electronic** distribution only recording medium 251, and generates a temporary key Ktemp)) (session key) to be shared with the extension section 263 and the **electronic** distribution only recording medium 251, if necessary.

The encryption/decryption module 275 is composed of a decryption unit 280, an encryption unit 281, a random... ...extension section 263 is composed of a mutual authentication module 290, a key encryption module 291, a decryption module 292, an extension module 293, an **electronic** watermark addition module 294, and a storage module 295. Since the mutual authentication module 290, the key decryption module 291, the decryption module 292, the extension module 293, the **electronic** watermark addition module 294, and the storage module 295 have functions similar to those of the mutual authentication module 101, the key decryption module 102, the decryption module 103, the extension module 104, the **electronic** watermark addition module 105, and the storage module 106 of the home server 51 respectively, their descriptions are omitted.

In addition, the **electronic** distribution only recording medium 251 is made to execute purchase processing to prepare charge information, and hold the prepared charge information, and is composed of... ...if necessary. Further, since details of the tamper check processing were described in Figures 68 to 71, their descriptions are omitted.

Here, in such an **electronic** distribution only recording medium 251, a save key Ksave)) peculiar to the **electronic** distribution only recording medium 251 is held by the storage module 311 of the encryption processing section 301. In the **electronic** distribution only recording medium 251, when the content key Kco)) is recorded in the external memory 303, the content key Kco)) is encrypted by the... ...to an encryption processing section that has encrypted a content key Kco)) to be recorded in the recording medium), whereas the contents recorded in the **electronic** distribution only recording medium 251 can be reproduced by any apparatus as far as it has a configuration similar to that of the above-mentioned... ...250 even if it does not hold a save key Ksave)).

Incidentally, in such a record reproduction apparatus 250, since contents are recorded in the **electronic** distribution only recording medium 251 together with the content key Kco)) by executing purchase processing, the record reproduction apparatus 250 can be configured without using... ...262 and the extension section 263 for the purpose of only recording the contents.

In addition, in such a record reproduction apparatus 250, since the **electronic** distribution only recording medium 251 is detachably provided, and contents can be reproduced from the **electronic** distribution only recording medium 251 that has recorded the contents and the content key Kco)) in another apparatus, the record reproduction apparatus 250 can be used without connecting to the **electronic** distribution service center 1 and the network 4 by having a reproduction function only.

However, in the user home network 5, when contents and a content key Kco)) are recorded in the **electronic** distribution recording medium 251 in the record reproduction apparatus 250 connected to the network 4 as described above, and the **electronic** distribution only recording medium 251 is used for reproducing the contents in a record reproduction not connected to the **electronic** distribution service center 1 or the network 4, it is possible that collection of charge information held by the **electronic** distribution only recording medium 251 is difficult in the **electronic** distribution service center 1.

Thus, in the **electronic** distribution only recording medium 251, for example, charge information in the storage module 311 is periodically retrieved from the control section 310 in the encryption processing section 301, and if there is uncollected charge information in the **electronic** distribution service center 1, contents can only be reproduced only one from purchase processing until the charge information is collected by applying reproduction limitation to corresponding contents, and at the same time, managed transfer of the contents is not performed as well.

In this way, in the **electronic music** distribution system 10, a user owning the **electronic** distribution only recording medium 251 is prevented from reproducing ...can be reproduced, if charge information is uncollected after the set time has passed since purchase processing, the contents cannot be reproduced. Further, in the **electronic** distribution only recording medium 251, limitation contents of the reproduction limitation may be held by associating it with charge information in the storage module 311 of the encryption processing section 301, or may be held by associating it with the **license** conditions information in the external membry 303. In addition, by storing reproduction limitation (the number of times or a period) in a handling policy and/or price information, at the time of purchase processing, the **electronic** distribution only recording medium 251 may take out information of the reproduction limitation from the handling policy and/or the price information, prepare **license** conditions information including this, and hold the prepared **license** conditions information in the external memory 303.

Here, purchase processing executed in the record reproduction apparatus 250 will be described using a flow chart shown... ...stored in the storage module 311 in the encryption processing section 301 via the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251, and if the delivery key Kd)) is effective, the processing proceeds to step S701.

In step S701, the upper controller... ...stored in the storage module 311 in the encryption processing section 301 via the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 has reached an upper limit set in advance, and if the total of the charges has not reached the upper... ...mass storage section 266, and transmits the read out public key certificate of the content provider 2 to the encryption processing section 301 in the **electronic** distribution only recording medium 251. Thus, in the encryption processing section 301 in the **electronic** distribution only recording medium 251, the control section 310 verifies a signature of the public key certificate of the content provider 2 in the signature... ...content provider secure container

in the mass storage section 266, and transmits the read out key data to the encryption processing section 301 in the **electronic** distribution only recording medium 251. Thus, in the encryption processing section 301 in the **electronic** distribution only recording medium 251, the upper controller 261 verifies a signature of the key data in the signature verification unit 324 in the encryption... ...content provider secure container in the mass storage section 266, and transmits the read out handling policy to the encryption processing section 301 in the **electronic** distribution only recording medium 251. Thus, in the encryption processing section 301 in the **electronic** distribution only recording medium 251, the control section 310 verifies a signature of the handling policy in the signature verification unit 324 in the encryption...mass storage section 266, and forwards the read out public key certificate of the service provider 3 to the encryption processing section 301 in the **electronic** distribution only recording medium 251. Thus, in the encryption processing section 301 in the **electronic** distribution only recording medium 251, the control section 310 verifies a signature of the public key certificate of the service provider 3 in the signature... ...service provider secure container in the mass storage section 266, and transmits the read out price information to the encryption processing section 301 in the **electronic** distribution only recording medium 251. Thus, in the encryption processing section 301 in the **electronic** distribution only recording medium 251, the control section 310 verifies a signature of the price information in the signature verification unit 324 in the encryption... ...inputting means 264, generates a purchase command corresponding to the selected and designated contents, and sends it to the encryption processing section 301 in the **electronic** distribution only recording medium 251. Thus, the control section 310 of the encryption processing section 301 generates charge information and **license** conditions information based on the handling policy (the handling policy whose signature was verified in step S704) and the price information (the price information whose... ...264 may be performed in advance prior to the purchase processing.

In step S708, the control section 310 in the encryption processing section in the **electronic** distribution only recording medium 251 saves the charge information (the charge information generated in step S707) in the storage module 311, and in the subsequent step S709, forwards the **license** conditions information (the **license** conditions information generated in step S707) to the external memory 303 via the external memory control section 302, thereby writing the **license** conditions information in the external memory 303. In addition, the **license** conditions information may be written in a tamper prevention region (as in the external memory of Figure 16) in the same manner as writing the data described above in Figure 69. Incidentally, the **license** conditions information may be saved in the storage module 311 of the encryption processing section 301 in the **electronic** distribution only recording medium 251.

In step S710, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 decrypts the encrypted individual key Ki)) included in the key data (the key data whose signature ware verified in the... ...using the save key Ksave)) in the encryption unit 321.

In step S711, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 forwards the content key Kco)) encrypted by the save key Ksave)) in step S710 to the external memory 303 via...
...content key Kco)) encrypted by the save key Ksave)) may be saved in the storage module 311 of the encryption processing section 301 in the **electronic** distribution only recording medium 251.

In step S712, the upper controller 261 in the record reproduction apparatus 250 reads out the encrypted contents included in the content provider secure container in the mass storage section 266, and forwards the read out encrypted contents to the **electronic** distribution only recording medium 251, thereby storing the encrypted contents in the external memory 303 in the **electronic** distribution only recording medium 251.

Incidentally, in the step S712, the upper controller 261 may save the handling policy whose signature was verified in corresponding...prior to saving the contents in the external memory 303.

Incidentally, if data is transmitted and received between the record reproduction apparatus 250 and the **electronic** distribution only recording medium 251, a signature is attached to the data on the transmission side, and the signature is verified on the receiving side.

As described above, the record reproduction apparatus 250 executes the purchase processing in the **electronic** distribution only recording medium 251, thereby recording the contents encrypted by the content key Kco)) in the external memory 303 of the **electronic** distribution only recording medium 251 and the content key Kco)) encrypted by the save key Ksave)) peculiar to the encryption processing section 301 of the **electronic** distribution only recording medium 251.

In addition, reproduction processing executed in the record reproduction apparatus 250 will be described with reference to a flow chart... ...of the contents that is instructed by a user via the inputting means 264 to be reproduced to the encryption processing section 301 in the **electronic** distribution only recording medium 251.

In step S721, by forwarding an ID of the contents given from the upper controller 261 to the external memory control section 302, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 reads out the encrypted content key Kco)) and **license** conditions information corresponding to the ID from the external memory 303 via the external memory control section 302, and forwards the read out encrypted content key Kco)) to the decryption unit 320 of the encryption/decryption module 315, and at the same time, forwards the **license** information to the control section 310. Further, the external memory control section 302 may perform tamper check in the similar manner as at the time of reading out data described above for Figure 68 when reading out the encrypted content key Kco)) and **license** conditions information from the external memory 303. Incidentally, in the **electronic** distribution only recording medium 251, the encrypted content key Kco)) and

the **license** conditions information may be held in the storage module 311 of the encryption processing section 301 and may be read out from the storage module... ...the ID of the contents in the storage module 311, and if the charge information corresponding to the ID has already been collected by the **electronic** distribution service center 1 and does not exist in the storage module 311, the processing proceeds to step S724.

In step S724, the control section 310 of the encryption processing section 301 updates the **license** conditions information, if necessary. That is, if utilization **right** contents included in the **license** conditions information is, for example, a number of times **right**, the control section 310 indicates to subtract the number of times of reproduction indicated by the number of times **right**. Then, the encryption processing section 301 saves the updated **license** conditions information in the external memory 303 via the external memory control section 302. At this point, the external memory control section 302 may perform tamper check as at the time of rewriting data described above for Figure 70. Incidentally, the **license** conditions information may be updated and saves in the storage module 311 of the encryption processing section 301.

Subsequently, in step S725, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 performs mutual authentication with the encryption processing section 262 of the record reproduction apparatus 250 using each other's mutual... ...described above for Figure 51, their detailed description are omitted.

In step S726, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 decrypts the encrypted content key Kco)) by the save key Ksave)) stored in the storage module 311 in the decryption... ...in step S625, and the processing proceeds to step S727.

In step S727, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording media 251 transmits the content key Kco)) encrypted by the temporary key Ktemp1)) to the encryption processing section 262 of the record... ...the control section 270 of the encryption processing section 262 in the record reproduction apparatus 250 takes the encrypted content key Kco)) transmitted from the **electronic** distribution only recording medium 251 in the decryption processing unit 280 of the encryption/decryption module 275, in step S725, decrypts the encrypted content ...decryption module 292 of the extension section 263 is at this point given the encrypted contents read out from the external memory 303 in the **electronic** distribution only recording medium 251 by the upper controller 261, decrypts the encrypted contents using the content key Kco)) given by the key decryption module... ...section 263 extends the contents given by the decryption module 292 by a predetermined method such as ATRAC, and forwards the extended contents to the **electronic** watermark addition module 294. In step S735, the **electronic** watermark module 294 of the extension section 263 inserts predetermined data such as an ID of the encryption processing section 301 of the **electronic** distribution only recording medium 251 instructed by the control section 270 of the encryption processing section 262 in the form of an **electronic** watermark in the extended contents given by the extension module 293.

Then, in step S736, by forwarding the contents obtained in the extension section 263 to, for example, a speaker (not shown), the upper controller 261 of the record reproduction apparatus 250 generates **music** based on the contents via the speaker. Thus, the record reproduction apparatus 250 can reproduce contents in this way.

Here, if charge information corresponding to... ...of the contents is stored in the storage module 311 in step S723, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 refers to the reproduction limitation at the time when charge information is uncollected in step S737, and determines whether or... ...is less than the number of times defined by the reproduction limitation), the processing proceeds to step S724, where the control section 310 updates the **license** conditions information, if necessary. Incidentally, the reproduction limitation to be used when chare information is uncollected may be held in the storage module 311 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 or the external memory 303, or may be stored in data of a handling policy or price information, or the like.

Incidentally, the **electronic** distribution only recording medium 251 may be provided in the home server 51 described above for Figure 15 or the fixed apparatus 52.

As described... ...although, in the record reproduction apparatus 250, the contents encrypted by the content key Kco)) and the content key Kco)) can be generated from the **electronic** distribution only recording medium 251 and the contents encrypted by the content key Kco)) can be decrypted by the content key Kco)), until charge information... ...in accordance with the reproduction limitation set in advance, and after the charge information is collected, the content can be utilized in accordance with utilization **right** contents purchased by the purchase processing.

In the above-mentioned configuration, the **electronic music** distribution system 10 is provided with the record reproduction apparatus 250 to which the **electronic** distribution only recording medium 251 is detachably inserted as an apparatus in the user home network 5, and when the contents encrypted by the content... ...delivery key Kd)) (i.e., a content provider secure container and a service provider secure container) are transmitted from the service provider 3, controls the **electronic** distribution only recording medium 251 by the record reproduction apparatus 250 to execute purchase processing, records the contents encrypted by the content key Kco)) in the **electronic** distribution only recording medium 251 in the external memory 303, and at the same time, decrypts the individual key Kl)) encrypted by the delivery key... ...by the individual key Kl)) by the individual key Kl)), and encrypts the decrypted content key Kco)) by the save key Ksave)) peculiar to the **electronic** distribution only recording medium 251 to record in the external memory 303. Incidentally, in the **electronic** distribution only recording medium 251, the save key Ksave)) is saved in the storage module 311 of the encryption processing section 301 having tamper resistant feature in the **electronic** distribution only recording medium 251.

In addition, by controlling the **electronic** distribution only recording medium 251 at the time of reproduction processing, the record reproduction apparatus 250 reads out the contents encrypted by the contents key... ...Ksave)) by the save key Ksave)), thereby taking out the contents encrypted by the content key Kco)) and the decrypted content key Kco)) in the **electronic** distribution only recording medium 251. Then, the record reproduction apparatus 250 decrypts the contents encrypted by the content key Kco)) using the content key Kco)) using the encryption processing section 262 and the extension section 263.

Therefore, in the **electronic music** distribution system 10, although the contents encrypted by the content key Kco)) and the content key Kco)) encrypted by the save key Ksave)) are recorded in the external memory 303 by the record reproduction apparatus 250 in the **electronic** distribution only recording medium 251, since the contents encrypted by the content key Kco)) and the decrypted content key Kco)) are read out from the **electronic** distribution only recording medium 251, it is not necessary to save a save key peculiar to the encryption processing section 262 in the record reproduction apparatus 250. Thus, in the **electronic music** distribution system 10, since other apparatuses different from the record reproduction apparatus 250 in which the **electronic** distribution only recording medium 251 records contents can reproduce the contents using the **electronic** distribution only recording medium 251 if the apparatuses have the encryption processing section 262 and the extension section 263 similar to those of the record reproduction apparatus 250, generality of the **electronic** distribution only recording medium 251 can be dramatically improved.

In addition, in the **electronic** distribution only recording medium 251, even if contents or a content key Kco)) is illegally read out from the external memory 303, by holding the... ...the save key Ksave)) can be prevented from being illegally read out, thereby enabling to prevent the contents from being illegally utilized.

Moreover, in the **electronic music** distribution system 10, due to the increased generality of the **electronic** distribution only recording medium 251, until charge information for contents recorded in the **electronic** distribution only recording medium 251, by limiting utilization of the contents (limiting a number of times and a period of reproduction and copying), illegal utilization of the contents can be prevented while the charge information is uncollected.

According to the above-mentioned configuration, a save key Ksave)) peculiar to the **electronic** distribution only recording medium 251 detachably inserted in the record reproduction apparatus 250 is held in the **electronic** distribution only recording medium 251, the record reproduction apparatus 250 transmits the contents encrypted by the content key Kco)), the content key Kco)) encrypted by the individual key Ki)), and the individual key Kl)) encrypted by the delivery key Kd)) to the **electronic** distribution only recording medium 251 at the time of purchase processing, and in the **electronic** distribution only recording medium 251, after recording the contents encrypted by the content key Kco)) in the external memory 303 and decrypting the encrypted individual... ...303, and takes out the contents encrypted by the content key Kco)) and the content key

Kco)) decrypted by the save key Ksave)) from the **electronic** distribution only recording medium 251 at the time of reproduction processing to decrypt the contents, thereby enabling reproduction of the contents from the **electronic** distribution only recording medium 251 even if the electronlc distribution only recording medium 251 is inserted in another record reproduction apparatus 250 different from the record reproduction apparatus 250 used for recording the contents, thus an **electronic music** distribution system that can dramatically increase generality of the **electronic** distribution only recording medium 251 can be realized.

Incidentally, in such an **electronic music** distribution system 10, the delivery key Kd)) is not held in the **electronic** distribution only recording medium 251, or the delivery key Kd)) is not used even if it is held, and after decrypting the content key Kco... ...contents by the record reproduction apparatus 250, the content key Kco)) may be encrypted using the temporary key Ktemp)) mutually authentication and shared with the **electronic** distribution only recording medium 251, and the content key Kco)) encrypted by the temporary key Ktemp)) may be transmitted to the **electronic** distribution only recording medium 251 together with the contents encrypted by the content key Kco)).

In addition, although the content provider 2 is applied as... ...the service provider 3 may be applied as the information transmission apparatus.

(8) Proxy processing of charge information and managed transfer processing of a utilization **right**

The **electronic** distribution only recording medium 251 described above for Figure 92, for example, when inserted in the home server 51 that is a management apparatus in the user home network 5 that is the data management system described above for Figure 15 as an apparatus to be connected to the **electronic** distribution service center 1, can transmit charge information held in the storage module 311 of the encryption processing section 301 to the home server 5, thus can cause the **electronic** distribution service center 1 to collect the charge information from the home server 51.

Thus, in the **electronic** distribution only recording medium 251, although, when holding charge information, for preventing illegal utilization of contents, a utilization **right** of the contents (a **right** for reproducing the contents) cannot be transferred to another apparatus (transfer with limitation, managed transfer) together with the contents, or deleted (deletion cannot be executed unless the charge processing is completed), when transmitting the charge information to the homes server 51 in this way, the utilization **right** of the contents can be transferred to another apparatus (transfer with limitation, managed transfer) together with the contents corresponding to the charge information in accordance with the transfer processing procedures of the managed transfer **right** described above for Figure 82.

Incidentally, when a utilization **right** of contents is transferred to another apparatus together with the contents from the **electronic** distribution only recording medium 251, an apparatus having obtained the contents and their utilization **right** can return the contents and their utilization **right** only to the **electronic** distribution only recording medium 251, if necessary. However, since the **electronic** distribution only recording medium 251 can be carried freely, it is sometimes difficult to easily return the contents and their utilization **right** from another apparatus.

Therefore, for example, the home server 51 (Figure 15) as an apparatus in the user home network 5 connected to the **electronic** distribution service center 1, when taking in charge information held in the **electronic** distribution only recording medium 251, takes in corresponding contents and their utilization **right** altogether from the **electronic** distribution only recording medium 251, and manages the taken in contents and their utilization **right** on behalf of the **electronic** distribution only recording medium 251.

Actually, proxy processing of charge information executed in the home server 51 and transfer (transfer with limitation, managed transfer) of a **right** (utilization **right**) for reproducing contents will be described with reference to a flow chart shown in Figure 95. In step S740, the **electronic** distribution only recording medium 251 is inserted in the home server 51, and when a user inputs an execution instruction of proxy processing of charge information and transfer processing of a utilization **right** via the inputting means 63 in this state, with the upper controller 62 controlling the home server 51 and the **electronic** distribution only recording medium 251, the control section 91 of the encryption processing section 65 in the home server 51 mutually authenticates with the encryption processing section 301 in the **electronic** distribution only recording medium 251 using each other's mutual authentication modules 95 and 314 and shares the temporary key Ktemp)).

Then, in step S741, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 forward the charge information held in the storage module 311 to the encryption unit 321 in the encryption/decryption module... ...information to which the signatures are attached to the upper controller 62 of the home server 51 via the communication section 300.

Incidentally, in the **electronic** distribution only recording medium 251, since a third party illegal obtains profit if charge information is tampered during transmission, a signature is always attached to... ...seen, the charge information may be sent without encryption. In the home server 51, proxy processing of charge information and transfer processing of a utilization **right** can be executed without using a handling policy and price information. Therefore, in the **electronic** distribution only recording medium 251, the handling policy and the price information may be transmitted to the home server 51, if necessary.

In step S742... ...upper controller 62 of the home server 51 forwards the charge information and the handling policy as well as the price information transmitted from the **electronic** distribution only recording medium 251 to the control section 91 of the

encryption processing section 65. Thus, the control section 91 verifies the signatures attached... ...the temporary key Ktemp)) by the temporary key Ktemp)).

Then, in step S743, the control section 310 of the encryption processing section 301 in the **electronic** distribution only recording medium 251 retrieves an ID of contents indicated by the charge information (the charge information transmitted to the home server 51 in... ...is unless deleted in the storage module 311) held in the storage module 311 at this point in step S742, and reads out all corresponding **license** conditions information and contents encrypted by the content key Kco)) from the external memory 303 via the external memory control section 302 based on the...content key Kco)) by the temporary key Ktemp)) in the encryption unit 321. Then, after attaching signatures to the content key Kco)) together with the **license** conditions information and the encrypted contents read out from the external memory 303 in the signature generation unit 323, the control section 310 transmits them to the homes server 51 via the communication section 300. Incidentally, signatures may be attached to the **license** conditions information, the contents and the content key Kco)) individually, or may be attached to the entirety of the **license** conditions information, the contents and the content key Kco)). Moreover, a signature may be attached to contents.

Subsequently, in step S744, the control section 91 of the encryption processing section 65 in the home server 51 takes in the **license** conditions information and the encrypted contents transmitted form the **electronic** distribution only recording medium 251 as well as the content key Kco)) encrypted by the temporary key Ktemp)) via the upper controller 62, and after verifying the signatures attached to the **license** conditions information and the encrypted contents as well as the content key Kco)) encrypted by the temporary key Ktemp)) in the signature verification unit 115... ...the ID of the encryption section (the ID of the encryption section of the apparatus that applied purchase processing to the contents) stored in the **license** conditions information (the **license** conditions information whose signature was verified in step S744) to its own ID (i.e., the ID of the encryption processing section 65 in the home server 51) to update the **license** conditions information.

Then, in step S747, the control section 91 of the encryption processing section 65 in the home server 51 encrypts the content key... ...by the save key Ksave)) held in the storage module 92 in the encryption unit 112 in the encryption/decryption module 96, and saves the **license** conditions information (the **license** conditions information updated in step S746) in the external memory 67 together with the encrypted content key Kco)) via the external memory control section 97...

18/K/8 (Item 3 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2009 European Patent Office. All rights reserved.

Country	Number	Kind	Date

Abstract ...and stores the same. Thus, contents purchased by an advance order can be actually purchased regardless of expiration dates of the distribution key. Furthermore, usage **right** is passed from a first information receiving device to a second information receiving device different in registration information at the tome of using contents. Thus...

Legal Status Type	Pub. Date	Kind	Text

Language

Fulltext Availability	Available Text	Language	Update	Word Count
Total Word Count (Document A)				
Total Word Count (Document B)				
Total Word Count (All Documents)				

Specification: ...a seller of contents to distribute contents safely to a user of the contents.
BACKGROUND ART

There are systems in which information (contents) such as **music** is encrypted and is sent to an information processing device of a user with whom a predetermined contract has been signed, and the user decrypts... ...resistant memory cited herein may be one that cannot be easily read out by a third party, and does not require a particular limitation in **terms** of hardware (for example, it may be a hard disk placed in an entrance-controlled room, a hard disk of a password-controlled personal computer, or the like) . A distribution key Kd)) required for encrypting a content key Kco)) is supplied in advance to the tamper memory 604 from an **electronic** distribution service center (not shown) and is stored therein.

For generating data to be passed to the content receiving device 620, the content sending device... ...encrypting portion 611 using this key. Also, the data encrypting portion 612 encrypts the content key Kco2)) using the distribution key Kd)) supplied from the **electronic** distribution service center (not shown). In this way, the second content sending device 610 sends the encrypted contents and the encrypted content key Kco2)) to... ...and it is impossible to understand how content users manipulate an apparatus, the tamper resistant memory cited herein needs to have internal data protected in **terms** of hardware, and thus the cipher processing portion 623 is a semiconductor chip having a structure that is hardly accessed from the outside, and has... ...difficult to read out data illegally from the outside. And, in the tamper resistant memory 627, the distribution key Kd)) supplied in advance from the **electronic** distribution service center (not shown) is stored.

In this connection, the tamper resistant memories 604, 614 of the content sending devices, 600, 610 are memories...thus making a configuration and receiving method of the content receiving device more complicated.

Also, an information receiving device that does not have content usage **right**, among information receiving devices that receive contents, can hardly use the contents.

Furthermore, information needed for using the distribution key Kd)) and the other contents... ...device, a playback method of the apparatus and a program storing medium in which even an information receiving device that does not have content usage **right**, among information receiving devices that use contents, can use the contents.

In the present invention, for solving such problems, the information receiving device having content usage **right** has the content key for decrypting the content data distributed from the information sending device, generates a playback command for another apparatus that does not have content data usage **right**, and sends again the generated playback command and the content key to another apparatus.

Thus, even in another apparatus that does not retain content playback **right**, the contents can be played using the playback command and the content key received from the information sending device which retains the contents.

Furthermore, the... ...or not the content data can be used among the plurality of information receiving devices, and a first information receiving device having content data usage **right** among the plurality of information receiving devices passes the usage **right** to a second information receiving device with which it is determined that the content data can be used.

Thus, among groups different from each other in registration information for using content data, it is made possible to use contents at the second information receiving device to which the usage **right** is passed from the first information receiving device, whereby the content data can be passed even among information receiving devices different from each other in... ...use by the user may be further improved.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing an entire configuration of an **electronic music** distribution system according to the present invention.

FIG. 2 is a block diagram showing a configuration of an **electronic** distribution service center.

FIG. 3 is a schematic diagram showing an example of a periodic update of a key.

FIG. 4 is a schematic diagram... ...a schematic diagram available for explanation of operations of an external memory controlling portion.

FIG. 17 is a block diagram showing a configuration of an **electronic** distribution-only recording medium.

FIG. 18 is a block diagram showing data contents possessed by each apparatus.

FIG. 19 is a block diagram showing data... ...of single contents.

FIG. 40 is a schematic diagram showing another example of price information of album contents.

FIG. 41 is a schematic diagram showing **license** condition information.

FIG. 42 is a schematic diagram showing accounting information.

FIG. 43 is a schematic diagram showing another example of the accounting information.

FIG. 44 is a schematic diagram showing a list of usage **right** contents.

FIG. 45 is a schematic diagram showing the usage **right**.

FIG. 46 is a schematic diagram showing single contents.

FIG. 47 is a schematic diagram showing album contents.

FIG. 48 is a schematic diagram showing...a processing procedure of playing back contents by the home server.

FIG. 74 is a flow chart showing a processing procedure of purchasing content usage **right** as a proxy by the home server.

FIG. 75 is a flow chart showing a processing procedure of changing contents of a user who has... ...FIG. 77 is a schematic diagram showing contents of rule part of price information.

FIG. 78 is a schematic diagram showing an example of changing **right** contents.

FIG. 79 is a flow chart showing a processing procedure of **redistributing content** usage **right**.

FIG. 80 is a flow chart showing a processing procedure of purchasing content usage **right** by the stationary apparatus.

FIG. 81 is a schematic diagram showing transition of rule part of **license** condition information.

FIG. 82 is a flow chart showing a processing procedure of transferring management transfer **right**.

FIG. 83 is a flow chart showing a processing procedure of giving back management transfer **right**.

FIG. 84 is a block diagram showing an information sending system according to the present invention.

FIG. 85 is a block diagram showing the information... ...flow chart showing a proxy purchase processing procedure when non-group apparatus performs accounting.

FIG. 91 is a block diagram showing another configuration of the **electronic music** distribution system.

FIG. 92 is a block diagram showing a configuration of the **electronic** distribution service center constituted by a personal computer.

FIG. 93 is a block diagram showing a configuration of the content provider constituted by the personal... ...one embodiment of the present invention will be described in detail with reference to the drawings.

(1) Information distribution system

FIG. 1 explains an EMD (**Electronic Music** Distribution) system 10 applying the present invention. Contents distributed to a user through this system is **digital** data with information itself having a value, and in the case of this example, one content corresponds to **music** data of one song. For contents, one content is provided as one unit (single), or multiple contents are provided as one unit (album) to the user. The user purchases contents (in fact, purchases **right** to use a content key Kco))), and uses the contents that is provided (in fact, decrypts the contents using the content key Kco)) and uses the same). Furthermore, of course, the invention is applicable not just to the sale of **music** data, but also to the sale of all the contents such as images and game programs.

An **electronic** distribution service center (END Service Center) 1 sends to content provider 2 an individual key K1)) and a public key certificate of the content provider... ...charge for use based on the accounting information, and performs processing of distributing benefits to the content provider 2, the service provider 3 and the **electronic** distribution service center 1 themselves.

The content provider 2 has digitized contents, inserts an **electronic** water mark into the contents for demonstrating that it is its own contents, compresses and encrypts the contents, generates a handling policy for the contents... ...the signature data thereto to send the same to the user home network 5 via a network 4 constituted by a dedicated cable network, an **internet** or satellite communication.

The user home network 5 obtains the contents sent from the service provider 3 with the price information added thereto, purchases content usage **right**, and carries out purchase processing. The usage **right** that is purchased may be, for example, playback usage **right** or replication **right**. And, the accounting information generated through purchase processing is stored in a tamper resistant memory in a cipher processing portion of the apparatus retained by the user, and is sent to the **electronic** distribution service center 1 when the user home network 5 obtains the distribution Kd)) from the **electronic** distribution service center 1.

FIG. 2 is a block diagram showing a configuration of a function of the **electronic** distribution service center 1. A service provider managing portion 11 supplies the public key certificate of the service provider 3 and information of benefit distribution...sends information showing a record of content usage of the user home network 5 to a group managing copyrights, for example JASRAC (Japanese Society for **Rights** of Authors, Composers and Publishers). A key server 14 performs generation, maintenance and management of the key for use in the entire system and for... ...Kd)) is supplied to the user home network 5 via a user managing portion 18. Also, all of the public key/secret key of the **electronic** distribution service center 1 and the public key/secrete key specific to the apparatus retained by the user are generated and managed, and the public... ...is unique to a cipher processing portion 92 described later may be generated and retained.

An example of periodic send of the key from the **electronic** distribution service center 1 to a home server 51 (described later) constituting the content provider 2 and the user home network 5 will be described referring to FIG. 3 to FIG. 6. FIG. 3 shows the distribution key Kd)) and individual key K1)) that the **electronic** distribution service center 1 has, the individual key K1)) that the content provider 2 has, and the distribution key Kd)) that the home server 51... ...Kd)) and the individual key Ki)) being version 6 can be used in June, 2000.

Before the content provider 2 starts to provide contents, the **electronic** distribution service center 1 sends to the content provider 2 the six individual keys Ki)) of version 1 to version 6 that can be used... ...encrypting contents and the content key Kco)) and so on before providing the contents.

Also, before the home server 51 starts to use contents, the **electronic** distribution service center 1 sends the three available distribution keys Kd)) being version 1 to version 3 to the home server 51 from January, 2000... ...despite the contracted period over which the contents can be purchased, due to the trouble that the home server 51 cannot be connected to the **electronic** distribution service center 1 because of the congested line and so on, and also for the purpose of reducing the frequency of connection to the

electronic distribution service center 1, and curbing simultaneous accesses by individual apparatuses to the **electronic** service center 1, thus reducing the load on the **electronic** distribution service center 1.

In the period of January 1, 2000 to January 31, 2000, the distribution key Kd)) and the individual key K1)) being version 1 are used at the **electronic** distribution service center 1, the content provider 2 and the home server 51 constituting the user home network 5.

Sending of the distribution key Kd)) and the individual key K1)) by the **electronic** distribution service center 1 to the content provider 2 and the home server 51 in February 1, 2000 will be described with reference to FIG. 4. The **electronic** distribution service center 1 sends to the content provider 2 the six individual keys K1)) of version 2 to version 7 that can be used... ...Kd)), which have been stored before the reception, and stores the new individual keys Ki)) and individual keys K1)) encrypted with distribution keys Kd)). The **electronic** distribution service center 1 sends to the home server 51 the three available distribution keys Kd)) being version 2 to version 4 from February, 2000... ...server 51 receives the three distribution keys Kd)), overwrites the distribution keys Kd)) stored before the reception, and stores the new distribution keys Kd)). The **electronic** distribution service center 1 directly stores the distribution keys Kd)) and the individual keys K1)) being version 1 to 7. This is for the purpose... ...period of February 1, 2000 to February 29, 2000, the distribution key Kd)) and the individual key K1)) being version 2 are used at the **electronic** distribution service center 1, the content provider 2 and the home server 51 constituting the user home network 5.

Sending of the distribution key Kd)) and the individual key K1)) by the **electronic** distribution service center 1 to the content provider 2 and the home server 51 in March 1, 2000 will be described with reference to FIG. 5. The **electronic** distribution service center 1 sends to the content provider 2 the six individual keys K1)) of version 3 to version 8 that can be used... ...Kd)), which have been stored before the reception, and stores the new individual keys K1)) and individual keys K1)) encrypted with distribution keys Kd)). The **electronic** distribution service center 1 sends to the home server 51 the three available distribution keys Kd)) being version 3 to version 5 from March, 2000... ...server 51 receives the three distribution keys Kd)), overwrites the distribution keys Kd)) stored before the reception, and stores the new distribution keys Kd)). The **electronic** distribution service center 1 directly stores the distribution keys Kd)) and the individual keys K1)) being version 1 to 8. This is for the purpose... ...period of March 1, 2000 to March 31, 2000, the distribution key Kd)) and the individual key Ki)) being version 3 are used at the **electronic** distribution service center 1, the content provider 2 and the home server 51 constituting the user home network 5.

Sending of the distribution key Kd)) and the individual key K1)) by the **electronic** distribution service center 1 to the content provider 2 and the home server 51 in April 1, 2000 will be described with reference to FIG. 6. The **electronic** distribution service center 1 sends to the content provider 2 the six individual keys K1)) of version 4 to version 9 that can be used... ...Kd)), which have been stored before the reception, and stores the new individual keys K1)) and individual keys Ki)) encrypted with distribution

keys Kd)). The **electronic** distribution service center 1 sends to the home server 51 the three available distribution keys Kd)) being version 4 to version 6 from April, 2000... ...server 51 receives the three distribution keys Kd)), overwrites the distribution keys Kd)) stored before the reception, and stores the new distribution keys Kd)). The **electronic** distribution service center 1 directly stores the distribution keys Kd)) and the individual keys Ki)) being version 1 to 9. This is for the purpose... ...period of April 1, 2000 to April 30, 2000, the distribution key Kd)) and the individual key K1)) being version 4 are used at the **electronic** distribution service center 1, the content provider 2 and the home ...even if he or she has made no access to the center for one or two months.

A background data managing portion 15 of the **electronic** distribution service center 1 (FIG. 2) retains and manages accounting information that is information showing the usage record of the contents collected by the user... ...and the content provider 2 if required data is already written in the accounting information. A benefit distributing portion 16 calculates the benefits of the **electronic** distribution service center 1, the content provider 2 and the service provider 3, based on the accounting information, and the price information and the handling... ...contents of the database. When the user home network 5 is constituted by a plurality of apparatuses having functions that can be connected to the **electronic** distribution service center 1, the user managing portion 18 defines an apparatus for which settlement is made in the registration information and registers the settlement... ...representing the ID of the group, and IDs specific to apparatuses constituting the home network 5, and information of whether or not connection to the **electronic** distribution service center 1 is possible, whether or not settlement processing is possible, whether or not the contents can be purchased, which apparatus performs settlement... ...this group unit. Therefore, in principle, a representative apparatus in the group performs on its own communication, settlement processing and update of information with the **electronic** distribution service center 1, and other in the group do not perform transactions directly with the **electronic** distribution service center 1. The IDs recorded in the user registration database are used for identifying an apparatus with the ID assigned individually for each apparatus.

Information of whether or not connection to the **electronic** distribution service center 1 recorded in the user registration database is possible shows whether or not the apparatus can be physically connected to the **electronic** distribution service center 1, and even an apparatus recorded as connectable one is not connected to the **electronic** distribution service center 1 in principle, unless it is considered to be capable of settlement processing (However, it may be connected to the **electronic** distribution service center 1 as a proxy on a temporary basis if the representative apparatus in the group becomes unable to perform settlement processing operations for some reason). Also, the apparatus recorded as an apparatus that is not connectable outputs accounting information and the like to the **electronic** distribution service center 1 via the apparatus capable of settlement processing in the user home network 5.

The information of whether or not settlement processing... ...the apparatus is capable of settlement processing. When the user home network 5 is constituted by a plurality of apparatuses capable of purchasing content usage **right** and so on, one apparatuses of

them that is capable of settlement processing sends to the **electronic** distribution service center 1 the accounting information, and the price information and the handling policy, as required, of all the apparatuses registered in the **electronic** distribution service center 1 of the user home network 5, and receives the distribution key Kd)) and the registration information from the **electronic** distribution service center 1 in response to completion of the settlement processing. In this way, processing at the **electronic** distribution service center 1 is alleviated, compared to performing processing for each apparatuses.

The information of whether or not purchase processing is possible, which is recorded in the user registration database, represents whether or not the apparatus is capable of purchasing content usage **right**. The apparatus that is not capable of purchasing the **right** has proxy purchase of usage **right** (which means that the apparatus has usage **right** purchased by another apparatus and receives all the **right**. The supplier retains no **right**), redistribution (a system in which content usage **right** that has been already purchased is purchased again in the same contents of usage **right** or the different contents of usage **right**. At this time, the supplier retains no **right**. Redistribution is mainly intended to give discounts. Only groups using the same settlement ID can receive benefits of discounts. Because for processing in the group belonging to the same settlement ID, a burden of processing on the **electronic** distribution service center 1 is reduced, and thus the discount can be received for it), or management transfer (Although content playback **right**, particularly an open-ended playback **right** can be transferred, at a playback **right** sender, which apparatuses is a playback **right** receiver is managed, and management transfer cannot be performed again if the playback **right** is not given back, and at the playback **right** receiver, which apparatuses is the playback **right** sender is managed, and management transfer cannot be performed at all, and the playback **right** can only be given back to the playback **right** sender which has given the playback **right**) performed by another apparatus capable of purchasing the **right** to obtain the content usage **right**.

Now, using methods/usage **right** of contents and methods of purchasing contents will be briefly described. For content using methods, there are two methods, a method in which those who manage and retain content usage **right** on their own use the contents, and a method in which they execute usage **right** retained by another apparatus to use the contents at their own apparatuses. Content usage **rights** include open-ended playback **right** (The period and the number of times for playing back contents are not limited, and contents are played back in the case of **music** contents, but contents are run in the case of game programs and the like), playback **right** with limit on time (The period over which the contents can be played is limited), playback **right** with limit on the number of times (The number of times for playing the contents is limited), open-ended replication **right** (The period and the number of times for replicating the contents are not limited), replication **right** with limit on the number of times (The number of times for replicating the contents is limited) (The replication **right** includes replication **right** without copy management information, replication **right** with copy management information (SCMS) and the like, and in addition, replication **right** for dedicated media and the like) (Also, there may be replication **right** with limit on time), and management transfer **right**. And, methods of purchasing usage **right** include, in addition to normal purchase to purchase these usage **rights** directly, change of the usage **right** contents to change the contents of

usage **right** already purchased to other contents, redistribution to purchase usage **right** separately based on the **right** already purchased by another apparatus, proxy purchase to have usage **right** purchased by another apparatus as a proxy, and album purchase to purchase and manage a plurality of content usage **rights** together.

Information described by the proxy settler recorded in the user registration database shows the ID of the apparatus that sends to the **electronic** distribution service center 1 as a proxy the accounting information generated when content usage **right** is purchased.

Information described by proxy purchasers recorded in the user registration database shows the ID of the apparatus that purchases usage **right** as a proxy for the apparatus that is not capable of purchasing usage **right**. However, in the case where all apparatuses in the group that are capable of purchase processing are proxy purchasers, record is not necessarily made.

Information... ...cases, use of purchased contents may be limited (However, there may be cases where the apparatus is registered again after it is brought in the **electronic** distribution service center 1 and the like and is checked). Also, in addition to "registration possible" and "registration impossible", there may be state of "unfinished...of functions of the content provider 2. A content server 31 stores contents to be supplied to the user and supplies the contents to an **electronic** watermark adding portion 32. The **electronic** watermark adding portion 32 inserts content provider ID representing its property into the contents supplied from the content server 31 in the form of **electronic** watermark, and supplies the same to a compressing portion 33. The compressing portion 33 compresses the contents supplied from the **electronic** watermark adding portion 32 by a system such as ATRAC (Adaptive Transform Acoustic Coding) (Trademark), and supplies contents to a content encrypting portion 34. In... ...required. The content key encrypting portion 36 encrypts the key Kco)) by the common key encryption system, using the individual key K1)) supplied from the **electronic** distribution service center 1, and outputs the result thereof to the signature generating portion 38. In this connection, the encryption system is not limited to...portion 38 in response to the contents to be encrypted. Furthermore, the handling policy generating portion 37 may supply the generated handling policy to the **electronic** distribution service center 1 via communicating means not shown in the figure, and the data thereof is retained and managed. The signature generating portion 38 adds **electronic** signatures to the encrypted contents, the encrypted content key Kco)), the encrypted individual key K1)) and the handling policy, and sends the same together with... ...the service provider 3 (Hereinafter, the encrypted contents, the encrypted content key Kco)), the encrypted individual key K1)) and the handling policy to which the **electronic** signatures are added respectively using the secret key of the content provider 3 are referred to as content provider secure container). Furthermore, instead of adding a signature to individual data separately, one signature may be added to the entire data.

A cross authenticating portion 39 performs cross authentication with the **electronic** distribution service center 1, and also performs cross authentication with the service provider 3 as required prior to the sending of the content provider secure... ...the memory 40A is a tamper resistant memory which is not vulnerable to readout of data by a third

party, but no particular limitation in **terms** of hardware is required (for example, it maybe a hard disk placed in an entrance-controlled room, a hard disk of a password-controlled personal... ...the signature using an elliptic curve cipher that is a public key cryptosystem. This processing will be described using FIG. 10 (EC-DSA (Elliptic Curve **Digital** Signature Algorithm), IEEE P1363/D). In Step S1, M is defined as a massage, p as a characteristic number, a and b as coefficients of...memory not shown in the figure (similar to 40A in the content provider 2) (Hereinafter, the content provider secure container and price information to which **electronic** signatures are added using the secret key of the service provider 3 is referred to as a service provider secure container). Furthermore, in stead of... ...3 are supplied to the user home network 5 via the network 4 (FIG. 1). A cross authenticating portion 46 performs cross authentication with the **electronic** distribution service center 1, and also performs cross authentication with the content provider as required, and with the user home network 5 if possible via the **internet**, cable communication and the like.

FIG. 15 is a block diagram showing a configuration of the user network 5. The home server 51 receives a secure container containing contents from the service provider 3 via the network 4, purchases content usage **right**, and executes the **right** to perform decryption, extension, playback and replication of contents.

A communicating portion 61 communicates with the service provider 3 or the **electronic** distribution service center 1 via the network 4, and receives or sends predetermined information. A host controller 62 receives a signal from inputting means 63, displays a predetermined message and the like on displaying means 64, performs processing such as the purchase of content usage **right** using a cipher processing portion 65, supplies the encrypted contents read out from a large capacity storing portion 68 to an extending portion 66, and... ...may be integrated into one device. The cipher processing portion 65 performs cross authentication with the cipher processing portion of the service provider 3, the **electronic** distribution service center 1 or other apparatuses to purchase content usage **right**, and performs encryption/decryption of predetermined data, manages an external memory retaining the content key Kco)) and **license** condition information, and stores the distribution key Kd)), accounting information and the like. The extending portion 66 performs cross authentication with the cipher processing portion... ...supplied from the host controller 62, using this content key Kco)), extends the contents with a predetermined system such as ATRAC, and inserts a predetermined **electronic** watermark into the contents. The external memory 67 is constituted by a nonvolatile memory such as a flash memory and a volatile memory with backup power, and stores the content key Kco)) encrypted with the save key Ksave)) and **license** condition information. The large capacity storing portion 68 is a storage device such as a HDD and an optical memory disk, and stores the content... ...policy, price information and their signatures), the public key certificate, registration information and the like.

The cipher processing portion 65 performing cross authentication with the **electronic** distribution service center 1, purchasing content usage **right** and generating accounting information, carrying out decryption/encryption of predetermined data, managing the external memory retaining the content key Kco)) and **license** condition information, and

storing the distribution key Kd)), accounting information and the like is constituted by a controlling portion 91, a memory module 92, a...performed, whether or not accounting information is passed, and whether or not redistribution of the contents is performed. The purchase processing module 94 newly generates **license** condition information from the handling policy and price information contained in the secure container received from the service provider 3 (and in some cases, **license** condition information already stored) and outputs the **license** condition information to the external memory controlling portion 97 or the controlling portion 91, and generates accounting information and outputs the same to the memory module 92. The cross authentication module 95 carries out cross authentication with the **electronic** distribution service center 1, and the cipher processing portion and the extending portion 66 of other apparatuses in the home network 5, and generates a... ...portion, and outputs the result thereof to the controlling portion 91. Furthermore, a method for generating/verifying a signature is similar to those described in **terms** of FIG. 10 and FIG. 11.

The external memory controlling portion 97 controls the external memory 67 to perform read and write of data, and... ...in the memory module 92. The external memory 67 is divided into N blocks of data areas, and M pairs of content keys Kco)) and **license** condition information can be written in each data area. Also, in the external memory 67, other areas that can be freely used are prepared. The... ...writing of the external memory will be described later, using flowcharts.

The extending portion 66 (FIG. 15) decrypting and extending contents and adding a predetermined **electronic** watermark thereto is constituted by a cross authentication module, a key decryption module 102, a decryption module 103, an extension module 104, an **electronic** watermark adding module 105 and a memory module 106. The cross authentication module 101 performs cross authentication with the cipher processing portion 65, and outputs... ...the extension module 104. The extension module 104 further extends the decrypted contents with a system such as ATRAC, and outputs the contents to the **electronic** watermark adding module 105. The **electronic** watermark adding module 105 inserts the individual ID of the cipher processing portion subjected to purchase processing into the contents, using an **electronic** watermark technique, outputs the same to a speaker not shown in the figure, and has **music** played back.

In the storage module 106 is stored key data that is needed for cross authentication with the cipher processing portion 65. Furthermore, it is desired that the extending portion 66 has tamper resistance.

The external memory 67 stores **license** condition information which is generated when the **right** is purchased at the purchase processing module 94 and the content key Kco)) encrypted with the save key Ksave)). The large capacity storing portion 68...of the external memory 67, and explanations thereof are thus omitted. The recording medium 80 is, for example, a MD (Mini Disk: Trademark) or an **electronic** distribution-only storing medium (memory stick using a semiconductor memory: Trademark).

A portable device 53, a device that the user carries and uses for playing back **music** with enjoyment, is constituted by a communication portion 81, a host controller 82, a cipher processing portion 83, an extending portion 84 and an external... ...not limited only to semiconductor memories, but may any of HDDs, rewritable optical disks and the like.

FIG. 17 is a block diagram of an **electronic** distribution-only recording medium. A recording medium 120 storing electronically distributed contents is constituted by a communicating portion 121, a cipher processing portion 122 and... ...portion 76 of the stationary apparatus 52 (FIG. 15). The cipher processing portion 122 performing cross authentication with the stationary apparatus 52, receiving content usage **right**, decrypting/encrypting predetermined data, managing the external memory that retains the content key Kco)), **license** condition information and the like, and further storing the save key Ksave)) and the like has a configuration having same functions as those of the... ...omitted. The external memory 123 stores the content key Kco)) encrypted with the save key Ksave)), the contents encrypted with the content key Kco)) and **license** condition information defining conditions for using the contents, and the handling policy and price information as required.

The **electronic** distribution-only recording medium 120 is different in usage from the recording medium described with the stationary apparatus 52. The normal recording medium 80 is a substitute for the large capacity storing portion 68 of the home server 51 while the **electronic** distribution-only medium 120 is not different from a portable device that does not have an extending portion. An apparatus such as the stationary apparatus 52 having the extending portion 74 is thus needed for playing back contents, but in **terms** of functions such as receipt of contents and management of contents, processing as in the case of the home server 51 and the portable device... ...the normal medium 80 can not be played back by apparatuses other than those that have recorded the contents, but the contents recorded in the **electronic** distribution-only recording medium 120 can be played back by apparatuses other than those that have recorded the contents. That is, since the normal recording... ...key Kco)), contents can not be played back with apparatuses other than those having (recording) the content key Kco)). On the other hand, in the **electronic** distribution-only recording medium 120, not only the contents encrypted with the content key Kco)) but also the content key Kco)) which is encrypted with the save key Ksave)) specific to the **electronic** distribution-only recording medium 120 is retained, thus enabling other apparatuses to play back the contents.

That is, cross authentication between a cross authentication module...may be unnecessary because of being included in registration information), secret keys different for each apparatus, the save key Ksave)), the public key of the **electronic** distribution service center 1 that is used when performing cross authentication with the **electronic** distribution service center 1 (which is unnecessary if there is the public key certificate of the **electronic** distribution service center 1), the public key of the authenticator station 22 for verifying the public key certificate, and the common key which is used... ...portion 65. These data are data that are stored in advance when apparatuses are manufactured. In contrast, the distribution key Kd)) distributed periodically from the **electronic** distribution service center 1, accounting information written when purchase processing is

performed, the content key Kco)) retained in the external memory 67, and the hash value for checking tamper of **license** condition information are data that are stored after use of the apparatus is started, and these data are also stored in the memory module 92... ...external memory 67 are stored the content key Kco)) encrypted with the save key Ksave)) that is used when the contents are decrypted, and the **license** condition information showing conditions when the content key Kco)) is used. Also, in the large capacity storing portion 68 are stored the certificate of the... ...portion 83 are stored individual IDs for identifying apparatuses, the secret key different for each apparatus, the save key Ksave)), the public key of the **electronic** distribution service center 1, which is used when performing cross authentication with the **electronic** distribution service center 1 (However, it is not necessary to have all procedures with the **electronic** distribution service center 1 performed by the home server 51 as a proxy), the public key of the authenticator station 22 for verifying the public... ...in advance when apparatuses are manufactured. Also, the content key Kco)) retained in the external memory 85 and the hash value for checking tamper of **license** condition information, and the ID for settlement as required, the distribution key Kd)) and (part of) registration information (In the case where purchase processing is... ...signature thereof may also be stored), the content key Kco)) encrypted with the save key Ksave)) that is used when the contents are decrypted, and **license** condition information showing conditions when the contents are used. Also, the public key certificate of the content provider 2 and the public key certificate of... ...addition to the configuration of the home server 51. The recording medium 80 may be a normal MD and CD-R, or may be an **electronic** distribution-only recording medium. In the case of the former, data to be recorded are decrypted contents with a copy prohibition signal added thereto but...storing the contents. For the save key Ksave)) is different for each apparatus).

Also, FIG. 19 can be considered as the recording medium. In the **electronic** distribution-only recording medium 120, individual IDs of the recording medium, the secret key different for each recording medium, the certificate of the public key... ...the external memory 123), the save key Ksave)) used for encrypting the content key Kco)) (generally, different for recording medium), the public key of the **electronic** distribution service center 1 (needless if exchange with the center is not performed, or there exist the public key certificate of the **electronic** distribution service center 1 in the external memory 123), the public key of the authenticator station, the hash value for checking tamper of the external... ...external memory 123, contents encrypted with the content key Kco)) (and the signature thereof) , the content key Kco)) encrypted with the save key Ksave)) and **license** condition information are stored, and the handling policy (and the signature thereof), price information (and the signature thereof), the public key certificate of the content... ...the public key certificate of the service provider 3 are stored as required.

FIG. 20 and FIG. 21 explain information sent and received among the **electronic** distribution service center 1, the content provider 2, the service provider 3 and the user home network 5. The content provider 2 adds the public... ...provider 3. Also, the content provider 2 sends the handling policy and the signature thereof, and the certificate of the content provider 2 to the **electronic** distribution service center 1 as required.

The service provider 3 verifies the public key certificate of the content provider 2, obtains the public key of... ...service provider 3 sends the price information and the signature as required thereof and the public key certificate of the service provider 3 to the **electronic** distribution service center 1.

The user home network 5 verifies the received secure container, and then performs purchase processing based on the handling policy and price information included in the secure container, generates accounting information and stores the same in the memory module in the encrypting processing portion, generates **license** condition information, decrypts the content key Kco)) and re-encrypts the same with the save key Ksave)), and stores the **license** condition information and the re-encrypted content key Kco)) in the external memory 67. And, in accordance with the **license** condition information, the content key Kco)) is decrypted with the save key Ksave)) and the contents are decrypted with this key for use. The accounting information is encrypted with the temporary key Ktemp)) in predetermined timing, and is provided with the signature, and is sent to the **electronic** distribution service center 1 together with the handling policy and price information as necessary.

The **electronic** distribution service center 1 calculates a usage charge based on the accounting information and the price information, and calculates benefits of the **electronic** distribution service center 1, the content provider 2 and the service provider 3, respectively. The **electronic** distribution service center 1 further compares the handling policy received from the content provider 2, the price information and as required, the handling policy received... ...the handling policy or illegal price addition has occurred in the service provider 3 or the user home network 5, and so on.

Furthermore, the **electronic** distribution service center 1 sends the public key certificate of the content provider to the content provider 2, and sends the public key certificate of...by the content provider 2 for each of single contents and each of album contents, and the user home network 5 shows the contents of **right** that can be purchased.

In the data of the handling policy for the single contents (FIG. 33) are stored a data type, the type of... ...an area code, usable apparatus conditions, usable User conditions, the ID of the service provider, generation management information, the number of rules including purchasable usage **right** indicated by the handling policy, address information indicating the position for storing the rule, the rule stored at the position indicated by the address information, the public key certificate, and the signature.

And, the rule is constituted by a rule number added as a reference number for each usage **right**, a usage **right** content number indicating the contents of usage **right**, its parameter, a minimum selling price, an amount of benefits of the content provider, a rate of benefits of such content provider, a data size... ...handling policy of the single contents stored at the position indicated by such address information, generation management information, the number of rules including purchasable usage **right** indicated by such handling policy, address information indicating the position for storing the rule, the rule stored at the position indicated by the address information... ...rule of the handling policy of the single

contents, the rule is constituted by a rule number added as a reference number for each usage **right**, a usage content number, a parameter, a minimum selling price, an amount of benefits of the content provider, a rate of benefits of such content...is created and the key for use in verification of the signature are included in the public key certificate.

Also, in the rule, the usage **right** content number is a number added for each usage **right** contents, and the parameter represents a parameter of the **right** contents. The minimum selling price represents a minimum selling price when the single and album contents are sold in accordance with the usage **right** contents, and the amount and rate of benefits of the content provider represent an amount of benefits and a rate of benefits to the selling... ...a data size of sending information, and such sending information is constituted by points to be added to the user from the purchase of usage **right**, defined by the content provider, mile information consisting of discounts appropriate to such points, and various kinds of information defined by the content provider 2... ...the handling policy represent purchase patterns of single contents in the album, in which each corresponding single contents can be purchased separately as a single **music** out of the album, or the corresponding single contents can be purchased only as an album **music** (That is, it can be purchased only together with other contents as an album).

Thus, the handling policy of the album contents are defined so that either the album contents or the single contents sellable as single **music** can be selected and purchased, such that the album contents are purchased based on rules of the handling policy of the album contents, or the single contents are purchased as a single **music** based on rules of the handling policy of the single contents.

Also, in the handling policy of the album contents, the signature is added to... ...handling policy of the single and album contents, since the amount and rate of benefits of the content provider may be managed together by the **electronic** distribution service center 1, the amount and rate of benefits of the content provider may be removed to make a configuration, as shown in FIG policy to which such price information is added, the number of rules including purchasable usage **right** indicated by such price information, address information indicating the position for storing the rule, the rule stored at the position indicated by the address information, the public key certificate, and the signature.

And, the rule is constituted by a rule number added as a reference number for each usage **right**, the amount of benefits of the service provider, the rate of benefits of the service provider, a price, a data size, and sending information.

Also... ...packet of the price information of the single contents stored at the position indicated by such address information, the number of rules including purchasable usage **right** indicated by such price information, address information indicating the position for storing the rule, the rule stored at the position indicated by such address information, the public key certificate, and the signature.

And, the rule is constituted by a rule number added as a reference number for each usage **right**, the amount of benefits of the service provider, the rate of benefits of the service provider, a price, a data size, and sending information, as... ...purchased, and the price represents the selling price of the single contents and album contents defined by the service provider 3 based on the usage **right** contents and the corresponding minimum selling price. The data size represents a data size of sending information, and such sending information is constituted by points to be added to the user from the purchase of usage **right**, defined by the service provider 3, mile information consisting of discounts appropriate to such points, and various kinds of information defined by the service provider 3 as necessary.

Here, when generating price information, the service provider 3 can define all purchasable usage **rights** indicated by the corresponding handling policy as the purchasable usage **right** indicated by such price information, and also define usage **right** selected optionally from all purchasable usage **rights** indicated by the handling policy as the purchasable usage **right** indicated by the price information, and can select the usage **right** defined by the content provider 2.

Also, in the price information of the album contents, a plurality of rules define selling prices appropriate to purchase patterns of album contents. Also, the rule of the price information of single contents that can be sold as single **music**, of price information of a plurality of single contents stored in the price information of the album contents, defines selling prices of single contents that can be sold as such single **music**.

Thus, in the price information of the album contents, adaptation is made so that the selling price of the album and the selling price of the single contents that can be purchased as single **music** can be recognized with such single price information.

Also, in the price information of the album contents, the signature is added to the whole, whereby... ...album, presence or absence of verification of the signature for the contents may be stored as in the case of the handling policy described in **terms** of FIG. 33 and FIG. 34. Also, in the price information of the album contents, the price information of plurality of single contents constituting the... ...price information of the single and album contents, since the amount and rate of benefits of the service provider may be managed together by the **electronic** distribution service center 1, the amount and rate of benefits of the service provider may be removed to make a configuration, as shown in FIG. 39 and FIG. 40.

FIG. 41 shows a data format of **license** condition information, and such **license** condition information is created based on the handling policy of the purchased contents when the user purchases the contents, in the apparatus of the user home network 5, and represents the usage **right** contents selected by the user of usage **right** contents indicated by this handling policy.

In the data of the **license** condition information are stored a data type, the type of **license** condition information, the expiration date of the **license** condition information, the ID of

the contents, the ID of the album, the ID of the cipher processing portion, the ID of the user, the... ...of the handling policy, the ID of the service provider, the ID of price information, the version of the price information, the ID of the **license** condition information, a rule number added to playback **right** (usage **right**) as a reference number, a usage **right** content number, the number of remaining playbacks, the expiration date of the playback **right**, a rule number added to replication **right** (usage **right**) as a reference number, a usage **right** content number, the number of remaining replications, generation management information, and the ID of the cipher processing portion retaining the playback **right**.

In the **license** condition information, the data type shows that this data is data of the **license** condition information, and the type of the **license** condition information shows which **license** condition information of single contents or album contents such **license** condition information is. The expiration date of the **license** condition information shows the period over which such **license** condition information is used, by a date on which the time period ends, or by the number of consecutive days between the specified date when starting to use the **license** condition information and the date when the expiration date is reached.

The ID showing the purchased single contents for the ID of the contents, and...
...contents.

Also, the ID of the content provider represents the ID of the content provider 2 that has defined the handling policy used for creating **license** condition information, and the ID of the handling policy indicates the handling policy used for creating such **license** condition information. The version of the handling policy indicates revision information of the handling policy used for creating the **license** condition information. The ID of the service provider represents the ID of the service provider 3 that has created price information used for creating the **license** condition information. The ID of the price information indicates price information used for creating such **license** condition information. The version of the price information indicates revision information of the handling policy used for creating the **license** condition information. Thus, by the ID of the content provider, the ID of the handling policy, the version of the handling policy, the ID of...
...information, the content provider 2 or the service provider 3 that has provided the content purchased by the user can be known.

The ID of **license** condition information is an ID that the cipher processing portion of the apparatus in the user home network 5 adds, and is used for identifying such **license** condition information. The rule number of playback **right** represents a reference number added to the playback **right** out of usage **right**, for which the rule number of the rule indicated by the corresponding handling policy and price information is used directly. The usage **right** contents represent the contents of playback **right** described later. The number of remaining playbacks represents the number of remaining playbacks out of the number of playbacks defined in advance for the purchased contents, and the expiration date of playback **right** indicates the period over which the purchased contents can be played back, with the date when the period ends, and so on.

Also, the rule number of replication **right** represents a reference number added to the replication **right** out of usage **right**, for which the rule number of the rule indicated by the corresponding handling policy and price information is used directly. The usage **right** contents represent the contents of replication **right** described later. The number of remaining replications represents the number of remaining replications out of the number of replications defined in advance for the purchased... ...information indicates the number of instances where contents can be repurchased when the contents are repurchased. The ID of the cipher processing portion possessing playback **right** indicates the cipher processing portion possessing playback **right** at this point in time, and the ID of the cipher processing portion possessing the playback **right** is changed when management transfer is performed.

In this connection, in the **license** condition information, the expiration date may be defined for replication **right**, and in the case where the expiration date is defined, the period over which the purchased contents can be replicated is indicated with the date... ...of the handling policy, the ID of the service provider, the ID of price information, the version of the price information, the ID of the **license** condition information, a rule number, the amount and rate of benefits of the content provider 2, the amount and rate of benefits of the service... ...information used for such purchase processing. The version of price information indicates revision information of the price information used for purchase processing.

The ID of **license** condition information represents the ID of the **license** condition information created at the time of purchase processing, and the rule number represents a rule number added as a reference number to purchased usage **right**. The amount and rate of benefits of content provider represent the amount and ratio to the sales of a dividend allocated to the content provider... ...and rate of benefits of the content provider, and the amount and rate of benefits of the service provider may be managed together by the **electronic** distribution service center 1, the amount and rate of benefits of the content provider and the amount and rate of benefits of the service provider may be removed to make a configuration, as shown in FIG. 43.

FIG. 44 shows contents of purchasable usage **right**, and such usage **right**, if broadly classified, includes playback **right**, replication **right, right** content changing **right**, repurchase **right**, additional purchase **right** and management transfer **right**.

The playback **right** includes open-ended playback **right** with no limit on the period and the number of times, playback **right** with limit on period in which there is limit on the playback period, playback **right** with limit on total time in which there is limit on total time of playback, and playback with limit on the number of times in which there is limit on the number of playbacks. The replication **right** includes open-ended replication **right** without copy management information, in which there is no limit on the period, no limit on the number of times, and no copy management information (for example, serial copy management: SCMS), replication **right** with limit on the number of times and without copy management information, in which there is limit on the number of replications but there is... ...information in which there is no limit on the period and the number of times

but copy management information is added and provided, and replication **right** with limit on the number of times and copy management information in which there is limit on the number of times and copy management information is added and provided. In this connection, the replication **right** includes, in addition, replication **right** with limit on the period in which there is limit on the period over which replication is possible (including replication **right** in which copy management information is added, and replication **right** in which such copy management information is not added), and replication **right** with limit on total time in which there is limit on total time of replication (namely, total time needed for playing back the replicated contents) (including replication **right** in which copy management information is added, and replication **right** in which such copy management information is not added), and so on.

Also, the **right** content changing **right** is a **right** to change the contents of usage **right** already purchased to other contents as described above, and the repurchase **right** is a **right** to purchase usage **right** separately based on the **right** purchased by another apparatus as described above. The additional purchase **right** is a **right** to purchase in addition to the contents already purchased separately other contents of the album including the contents to integrate them into an album, and the management transfer **right** is a **right** to transfer the purchased usage **right** to change the owner.

Now, specific examples of usage **right** contents as shown in FIG. 33 and the like. In fact, for the data of open-ended playback **right**, as shown in FIG. 45 (A), information of the expiration date of the playback **right** indicating the effective period of the playback **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and the day when the period ends, and so on, is stored in the region of the usage **right** contents. For the data of playback **right** with limit on the period, as shown in FIG. 45 (B), information of the playback **right** indicating the effective period of the playback **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and the day when the period ends, and so on, is stored in the region of the usage **right** contents.

For the data of playback **right** with limit on total time, as shown in FIG. 45 (C), information of the expiration date of the playback **right** indicating the effective period of the playback **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and... ...number of days and time indicating limit on the total time over which playback can be performed are stored in the region of the usage **right** contents. For the data of playback **right** with limit on the number of times, as shown in FIG. 45 (D), information of the expiration date of the playback **right** indicating the effective period of the playback **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and... ...and information of the number of playbacks indicating the number of instances where playback can be performed are stored in the region of the usage **right** contents.

Also, for the data of open-ended replication **right** without copy management information, as shown in FIG. 45 (E), information of the expiration date of the replication **right** indicating the effective period of the replication **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and the day when the period ends, and so on, is stored in the region of the usage **right** contents. For the data of replication **right** with limit on the number of times and without copy management information, as shown in FIG. 45 (F), information of the expiration date of the replication **right** indicating the effective period of the replication **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and... ...and information of the number of replications indicating the number of instances where replication can be performed are stored in the region of the usage **right** contents.

For the data of replication with copy management information, as shown in FIG. 45 (G), information of the expiration date of the replication **right** indicating the effective period of the replication **right** by the date on which the period ends, or by the number ...specified day when the effective period starts and the day when the period ends, and so on, is stored in the region of the usage **right** contents. For the data of replication **right** with limit on the number of times and copy management information, as shown in FIG. 45 (H), information of the expiration date of the replication **right** indicating the effective period of the replication **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and... ...period ends, and so on, and information of the number of instances where replication can be performed are stored in the region of the usage **right** contents.

Furthermore, for the data of **right** content changing **right**, as shown in FIG. 45 (I), information of the expiration date of the **right** content changing **right** indicating the effective period of the **right** content changing **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and the day when the period ends, and so on, a former rule number for retrieving the usage **right** contents before it is changed, and a new rule number for retrieving the usage **right** contents after it is changed are stored in the region of the usage **right** contents. In this connection, if solely considering the replication **right** with limit on the period, as the usage **right** contents, for example, two or more kinds of contents exist for each usage **right** contents so that two or more kinds of replication **rights** with limit on the period depending on the definition of the period. Thus, since the usage **right** contents can be hardly managed with the usage **right** content number alone, in the **right** content changing **right**, the usage **right** contents are managed with the rule number added for each plurality of contents.

For the data of repurchase **right**, as shown in FIG. 45 (J), information of the expiration date of the repurchase **right** indicating the effective period of the repurchase **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and the day when the period ends, and so on, a former rule number for retrieving the usage **right** contents before it is changed, a new rule number for retrieving the usage **right** contents after it is changed, and maximum

distribution generation information indicating the maximum number of instances where repurchase can be performed are stored in the region of the usage **right** contents.

For the data of additional purchase **right**, as shown in FIG. 45 (K), information of the expiration date of the additional purchase **right** indicating the effective period of the additional purchase **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and...
...contents of the single already purchased, out of a plurality of single contents constituting the album contents, are stored in the region of the usage **right** contents.

For the data of management transfer **right**, as shown in FIG. 45 (L), information of the expiration date of the management transfer **right** indicating the effective period of the management transfer **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and the day when the period ends, and so on, is stored in the region of the usage **right** contents.

In this connection, as the usage **right** contents, content purchase **right** to purchase contents in accordance with a predetermined order when data of games are divided into a plurality of contents may be defined, for example. And, for the data of content purchase **right**, as shown in FIG. 45 (M), information of the expiration date of the content purchase **right** indicating the effective period of the content purchase **right** by the date on which the period ends, or by the number of consecutive days between the specified day when the effective period starts and... ...when the period ends, and so on, the ID of the contents already purchased, a former rule number for retrieving the contents of the usage **right** that has been already purchased, and a new rule number for retrieving the contents of the usage **right** contents that is newly purchased are stored in the region of the usage **right** contents. In this way, it is possible to have game programs having consecutive stories and so on purchased by the user, and upgrade the contents... ...started and the day when the period ends, and so on. The category of the contents shows which category the contents belong to, such as **music** data, program data, image data, and the ID of the contents is for identifying these single contents.

The ID of the content provider represents the...the cross authentication is unsuccessful.

FIG. 53 explains operations when a settlement-capable apparatus in the user home network 5 sends accounting information to the **electronic** distribution service center 1. The settlement-capable apparatus in the user home network 5 retrieves from registration information a target apparatus for which proxy settlement... ...the accounting information sent (At this time, the signature is added to the data) . After processing is completed for all apparatuses, cross authentication with the **electronic** distribution service center 1 is performed, all the accounting information is encrypted with the shared temporary key, signature data is added to them, and they are sent to the **electronic** distribution service center 1, together with registration information, and the handling policy and price information as required. Furthermore, since information necessary for distribution of money... ...handling policy and the ID of price information is included in the accounting information which is sent from the user home network 5 to the **electronic** distribution

service center 1, the handling policy and price information with large amounts of information are not necessarily sent. The user managing portion 18 receives... ...to perform encryption with the temporary key Ktemp)) to prevent viewing from the outside. In contrast to this, in the case of accounting information and **license** condition information, since data cannot be used illegally even if their contents are viewed, encryption with the temporary key Ktemp)) is not necessarily performed, but if the money amount of accounting information is tempered and the usage condition of **license** condition information is tampered so that it is loosened, parties involved in acceptance of money will suffer a loss. Therefore, accounting information and **license** condition information are sent with the signature added thereto, thereby preventing tampering. However, the signature may also be added when the content key Kco)) and... ...processes including use, stop of purchase processing, states of processing normally performed and the like).

FIG. 54 explains operations of benefit distribution processing of the **electronic** distribution service center 1. The background data managing portion 15 ...user managing portion 18. The benefit distributing portion 16 calculates the benefit of each of the content provider 2, the service provider 3 and the **electronic** distribution service center 1 from the accounting information, and the handling policy and the price information as required, which have been sent from the background... ...in the data of the accounting information supplied from the apparatus in the user home network 5.

FIG. 55 explains operations of processing, of the **electronic** distribution service center 1, for sending a usage record of contents to JASRAC. The background data managing portion 15 sends accounting information indicating the user... ...a flow chart explaining processing to distribute and play back contents by this system. In Step S40, the content provider managing portion 12 of the **electronic** distribution service center 1 sends the individual key Ki)), the individual key K1)) encrypted with the distribution key Kd)), and the public key certificate of... ...the home server 51 in FIG. 15), and registers the apparatus of the user home network 5 in the user managing portion 18 of the **electronic** distribution service center 1. Details about this registration processing will be described later referring to the flow chart of FIG. 59. In step S42, the user managing portion 18 of the **electronic** distribution service center 1 performs cross authentication with the user home network 5 as described above with reference to FIG. 52, followed by sending the... ...processing will be described later referring to the flow chart of FIG. 72.

FIG. 57 is a flow chart explaining details about processing where the **electronic** distribution service center 1 sends to the content provider 2 the individual key K1)), the individual key Ki)) encrypted with the distribution key Kd)) and the public key certificate, and the content provider 2 receives them. In Step 550, the cross authenticating portion 17 of the **electronic** distribution service center 1 performs cross authentication with the cross authenticating portion 39 of the content provider 2. This cross authentication processing has been described... ...key Ki)), the individual key Ki)) encrypted with the distribution key Kd)) and the certificate sent from the content provider managing portion 12 of the **electronic** distribution service center 1, in Step S51. In Step S52, the content provider 2 stores the received individual key K1)) in the tamper resistant

memory...way, the content provider 2 receives the individual key Ki)), the individual key Ki)) encrypted with the distribution key Kd)) and the certificate from the **electronic** distribution service center 1. In a similar way, in the case of performing processing of the flow chart shown in FIG. 56, the service provider... ...from the individual key Ki)) of the content provider 2), the individual key K1)) encrypted with the distribution key Kd)) and the certificate from the **electronic** distribution service center using processes as in the case of FIG. 57.

Furthermore, the memory 40A retains the individual key K1)) that the content provider... ...thus it is desirably the tamper resistant memory in which data is not easily read out by a third party, but a particular limitation in **terms** of hardware is not required (For example, it may be a hard disk placed in an entrance-controlled room or a hard disk of a... ...memory.

FIG. 58 is a flow chart explaining processing where the home server 51 registers settlement information in the user managing portion 18 of the **electronic** distribution service center 1. In Step S60, the home server 51 performs cross authentication of the public key certificate stored in the large capacity storing portion 68 with the cross authenticating portion 17 of the **electronic** distribution service center 1, using the cross authentication module 95 of the cipher processing portion 65. This authentication processing is similar to that described referring to FIG. 52, and description thereof is thus omitted. The certificate which the home server 51 sends to the user managing portion 18 of the **electronic** distribution service center 1, in Step S60, includes the data shown in FIG. 32 (the public key certificate of the user apparatus).

In Step S61... ...These data are encrypted by the encryption unit 112 using the temporary key Ktemp)), and are sent to the user managing portion 18 of the **electronic** distribution service center 1 via the communicating portion 61.

In Step S63, the user managing portion 18 of the **electronic** distribution service center 1 fetches the ID of the apparatus from the received certificate, and retrieves the user registration database shown in FIG. 7 on the basis of this ID of the apparatus. In Step S64, the user managing portion 18 of the **electronic** distribution service center 1 determines whether or not it is possible to register the apparatus having the received ID, and if determining that it is... ...having the received ID is that of new registration, advancement to Step S66 is made.

In Step S66, the user managing portion 18 of the **electronic** distribution service center 1 newly issues a settlement ID, decrypts the settlement information encrypted with the temporary key Ktemp)), registers the settlement ID and the... ...information has been described with reference to FIG. 8, detailed description thereof is thus omitted.

In Step S68, the user managing portion 18 of the **electronic** distribution service center 1 sends the created registration information to the home server 51. In Step S69, the host controller 62 of the home server... ...These data are encrypted by the encryption unit 112 using the temporary key Ktemp)), and are sent to the user managing portion 18 of the

electronic distribution service center 1 via the communicating portion 61, along with the registration information already issued during settlement registration.

In Step S64, if it is... ...is not possible to register the apparatus having the received ID, advancement to Step S71 is made, and the user managing portion 18 of the **electronic** distribution service center 1 creates registration information of refused registration, and proceeds to Step S68.

In Step S65, if it is determine that the apparatus having the received ID is not that of new registration, procedures continue to Step S72, and the user managing portion 18 of the **electronic** distribution service center 1 decrypts the settlement information encrypted with the temporary key and register the information in the settlement information registration database with the way, the home server 51 is registered in the **electronic** distribution service center 1.

FIG. 59 is a flow chart explaining processing of performing new registration of the ID of the apparatus in the registration... ...S82 is similar to Step S64 in FIG. 58, and description thereof is thus omitted. In Step S83, the user managing portion 18 of the **electronic** distribution service center 1 defines a registration item corresponding to the apparatus ID in the user registration database as "registration", and registers the apparatus ID. In Step S84, the user managing portion 18 of the **electronic** distribution service center 1 creates registration information as shown in FIG. 8, based on the user registration database. Step S85 is similar to Step S68... ...that registration of the apparatus having the received ID is not possible, advancement to Step S87 is made, the user managing portion 18 of the **electronic** distribution service center 1 creates registration information of refused registration and proceeds to Step S85.

In this way, the home server 51 is registered in the **electronic** distribution service center 1.

FIG. 60 is a flow chart explaining processing where another apparatus is additionally registered via an apparatus which has been already... ...processing described with reference to FIG. 52, and description thereof is thus omitted. In Step S91, the home server 51 performs cross authentication with the **electronic** distribution service center 1. In Step S92, the home server 51 sends to the **electronic** distribution service center 1 the registration information read from the large capacity storing portion 68, and the certificate of the stationary apparatus 52 obtained when... ...S95 is same as step 83 in FIG. 59, and description thereof is thus omitted. In Step S96, the user managing portion 18 of the **electronic** distribution service center 1 newly creates registration information with information of the stationary apparatus 52 added to the registration information received from the home server... ...apparatus having the received ID is not possible in Step S94, advancement to Step S99 is made, and the user managing portion 18 of the **electronic** distribution service center 1 creates registration information meaning that only the stationary apparatus 52 is refused for registration (Therefore, the home server 51 remains registered), and proceeds to Step S97 (The home server 51 succeeds in cross

authentication with the **electronic** distribution service center 1, which means that registration of the home server 51 is possible).

Thus, the stationary apparatus 52 is registered additionally in the **electronic** distribution service center 1 through the processing procedure shown in FIG. 60.

Now, timing of update of registration (update of registration information) performed by the... ...has not passed since suction of the distribution key Kd)), registration information or accounting information, namely the update condition of registration information is satisfied in **terms** of passage of time, and the home server 51 proceeds to Step S601 at this time.

In Step S601, the home server 51 determines whether... ...processing, and in contrast to this, if a negative result is obtained, it means that the update condition of registration information is not satisfied in **terms** of the number of times contents have been purchased, and the home server 51 thus moves to the following Step S602.

In step S602, the to this, if a negative result is obtained in Step S602, it means that the update condition of registration information is not satisfied in **terms** of the amount of money spent for purchasing the contents, and the home server 51 moves to following Step S603.

In step S603, the home... ...In contrast to this, if a negative result is obtained in Step S603, it means that the update condition of registration information is satisfied in **terms** of the expiration date of the distribution key Kd)), and at this time, the home server moves 51 to following Step S604.

In Step S604... ...contrast to this, if a negative result is obtained in Step S604, it means that the update condition of registration information is not satisfied in **terms** of network configuration, and the home server 51 thus moves to following Step S605.

In Step S605, the home server 51 determines whether or not... ...of registration information has not been requested.

In Step 5606, the home server 51 performs update determination as in Step S600 to Step S605, in **terms** of other connected apparatuses, and proceeds to Step S607 to carry out processing to update registration information when a result showing that update should be... ...information and its signature, the handling policy, price information and registration information stored in the large capacity storing portion 68 are sent together to the **electronic** distribution service center 1. Furthermore, at this time, the handling policy and price information are not necessarily sent depending on a model. For there may be cases where the content provider 2 and the service provider 3 send them in advance to the **electronic** distribution service center 1, or cases where necessary information out of the handling policy and price information is included in the accounting information.

Step S102... ...S103 is same as Step S82 in FIG. 59, and description thereof is thus omitted. In Step S104, the user managing portion 18 of the **electronic** distribution service center 1 verifies the signature with the signature verification unit 115, decrypts the received accounting information with the temporary key Ktemp)) (In the case where the **electronic** signature is added to the received data, verification is performed with the signature verification unit 115), and (if it is already received) sends it to... ...The background data managing portion 15, which receives this, stores and manages the received data.

In Step S105, the user managing portion 18 of the **electronic** distribution service center 1 verifies the registration item corresponding to the ID of the apparatus in the user registration database, and updates the data. They... ...S106 is same as Step S84 in FIG. 59, and description thereof is thus omitted. In Step S107, the user managing portion 18 of the **electronic** distribution service center 1 encrypts with the temporary key Ktemp)) the distribution key Kd)) supplied from the key server 14, and sends the same to...Step S109, the home server 51 inputs the received registration information in the cipher processing portion 65, and the cipher processing portion 65 verifies the **electronic** signature included in the registration information with the signature verification unit 115, and has it checked that the apparatus ID of the home server 51... ...registration of the apparatus having the ID received is not possible, advancement to Step S111 is made, and the user managing portion 18 of the **electronic** distribution service center 1 creates registration information of refused registration and proceeds to Step S112. In Step S112, unlike Step S107, only the registration information... ...Step S113 is made to perform predetermined error handling.

In this way, the home server 51 updates registration information, and sends accounting information to the **electronic** distribution service center 1, for which it receives the distribution key Kd)) supplied.

FIG. 63 and FIG. 64 is a flow chart explaining processing where... ...In Step S124, the home server 51 performs cross authentication and shares the temporary key Ktemp)) 2 with the cross authenticating portion 17 of the **electronic** distribution service center 1. In Step S125, the home server 51 encrypts the accounting information sent from the stationary apparatus 52 with the encryption unit...signature, and the handling policy, price information and registration information corresponding to the accounting information as necessary to the user managing portion 18 of the **electronic** distribution service center 1.

In Step S126, the user managing portion 18 of the **electronic** distribution service center 1 retrieves the user registration database. In Step S127, whether or not the home server 51 and the stationary apparatus 52 are... ...and if it is determined that they are registered, advancement to Step S128 is made. In Step S128, the user managing portion 18 of the **electronic** distribution service center 1 verifies the signature for the accounting information encrypted with the temporary key Ktemp)) 2, and decrypts the accounting information with the... ...information, and the handling policy and price information if received, manages and stores those data.

In Step S129, the user managing portion 18 of the **electronic** distribution service center 1 updates the user registration database (the accounting data reception date, registration information issuance data, distribution key issuance date and the like not shown in the figure) . In Step S130, the user managing portion 18 of the **electronic** distribution service center 1 creates registration information (a case of FIG. 18, for example). In Step S131, the user managing portion 18 of the **electronic** distribution service center 1 encrypts with the temporary key Ktemp)) 2 the distribution key Kd)) received from the key server 14 of the **electronic** distribution service center 1, and generates the signature for the distribution key Kd)) encrypted with the temporary key Ktemp)) 2. And, the registration information, the... ...distribution key Kd)) encrypted with the temporary key Ktemp)), sends the same to the stationary apparatus 52 along with the registration information sent from the **electronic** distribution service center 1.

In Step S133, the host controller 72 of the stationary apparatus 52 overwrites the received registration information and stores it in... ...is similar to Step S130, and detailed description thereof is thus omitted. For Step S138, in Step S131, the user managing portion 18 of the **electronic** distribution service center 1 sends the registration information to the home server 51. In Step S139, the home server 51 sends the registration information to...service provider 3, which corresponds to Step S43 in FIG. 56 will be described, using a flow chart of FIG. 65. In Step S140, the **electronic** watermark adding portion 32 of the content provider 2 inserts predetermined data indicating the content provider 2, for example the content provider ID into the contents read from the content server 31 in the form of an **electronic** watermark, and supplies the same to the compressing portion 33. In Step S141, the compressing portion 33 of the content provider 2 compresses the contents with the **electronic** watermark inserted therein with a predetermined system such as ATRAC, and supplies the same to the content encrypting portion 34. In Step S142, the content... ...the content key encrypting portion 36. In Step S143, the content encrypting portion 34 of the content provider 2 encrypts the compressed contents with the **electronic** watermark inserted therein, with a predetermined system such as DES, using the content key Kco)).

In Step S144, the content key encrypting portion 36 encrypts the contents Kco)) with the individual key K1)) supplied from the **electronic** distribution service center 1, through the process of Step S40 in FIG. 56, using a predetermined method such as DES. In Step S145, the handling...51. Furthermore, these input processing may be performed when purchase processing is started. The cipher processing portion 65, which receives this, generates accounting information and **license** condition information from the handling policy inputted in Step S167 and the price information inputted in Step S169. The accounting information has been described with reference to FIG. 42, and description thereof is thus omitted. The **license** condition information has been described with reference to FIG. 41, and description thereof is thus omitted.

In Step S171, the controlling portion 91 of the... ...information generated in Step S170 in the memory module 92. In Step S172, the controlling portion 91 of the cipher processing portion 65 sends the **license** condition information ...in Step S170 to the external memory controlling portion 97 of the cipher processing portion 65. The external memory

controlling portion 97, which receives the **license** condition information makes a tamper check for the external memory 67, followed by writing the **license** condition information in the external memory 67. The tamper check at the time of writing it will be described later, using FIG. 69. In Step... ...the entire first block of FIG. 16). At this time, data other than the data due to be read (for example, content key 1 and **license** condition information 1) are discarded after they are used for calculation of the hash value. In step S182, the hash value calculated in Step S181...to the external memory controlling portion 97 of the cipher processing portion 65, and has the content key Kco)) corresponding to the content ID and **license** condition information retrieved. At this time, it confirms that the **license** condition information is a **right** capable of being regenerated. In Step S202, the external memory controlling portion 97 of the cipher processing portion 65 calculates the hash value of the data block including the content key Kco)) and the **license** condition information, and sends the hash value to the controlling portion 91 of the cipher processing portion 65. In Step S203, the controlling portion 91 S204, the controlling portion 91 of the cipher processing portion 65 updates the **license** condition information as necessary. For example, if usage **right** in the **license** condition information is represented by a coupon ticket, it is a process to subtract the number of counts of the coupon ticket, and so on. Thus, purchased **right** and the like requiring no update do not need to be updated, and in that case, a jump to Step S208 is made (not shown). In Step S205, the external controlling portion 97 rewrites and updates in the external memory 67 the updated **license** condition information sent from the controlling portion 91. In Step S206, the external memory controlling portion 97 calculates the hash value for all the data... ...module 104 of the extending portion 66 extends the contents with a predetermined system, for example a system such as ATRAC. In Step S215, the **electronic** watermark addition module 105 inserts data indicated from the cipher processing portion 65 into the contents in the form of an **electronic** watermark (Data passed from the cipher processing portion to the extending portion include not only the content key Kco)) but also playback conditions (analog output, **digital** output, output with copy controlling signals (SCMS)), the ID of the apparatus that has purchased content usage **right**, and so on. Data to be inserted is the ID of the apparatus that has purchased the content usage **right** (that is, the apparatus ID in the **license** condition information, and the like). In Step S216, the extending portion 66 plays back **music** via a speaker not shown in the figure.

In this way, the home server 51 plays back the contents.

FIG. 74 is a flow chart explaining a detailed process in which the home server 51 purchases content usage **right** as a proxy for the stationary apparatus 52. In step S220, the home server 51 and the stationary apparatus 52 perform cross authentication. Cross authentication... ...the signature authentication unit 115 of the encryption/decryption module 96 authenticate the signature added to the registration information, with the public key of the **electronic** distribution service center 1 supplied from the memory module 92 of the cipher processing portion 65. After success in authentication of the signature, the controlling... ...controlling portion 91 of the cipher processing portion 65 generates the signature for the content key Kco)) encrypted with the temporary key Ktemp)) and the **license** condition information generated in Step ...host controller 62. The

host controller 62 of the home server 51, which receives the content key Kco)) encrypted with the temporary key Ktemp)), the **license** condition information and their signatures, reads the contents encrypted with the content key Kco)) (Including signatures. Same in the following) from the large capacity storing portion 68, and sends the content key Kco)) encrypted with the temporary key Ktemp)), the **license** condition information, their signatures and the contents encrypted with the content key Kco)) to the stationary apparatus 52.

In Step S230, the stationary apparatus 52, which receives the content key Kco)) encrypted with the temporary key Ktemp)), the **license** condition information, their signatures and the contents encrypted with the content key Kco)), verifies the signature, followed by outputting the contents encrypted with the content... ...S232, the cipher processing portion 73 of the stationary apparatus 52 sends the content key Kco)) encrypted with the save key Ksave)) 2 and the **license** condition information received in Step S230 to the external memory controlling portion of the cipher processing portion 73, and has the same stored in the... ...has been already described with reference to FIG. 69, detailed description thereof is thus omitted.

In this way, the home server 51 purchases content usage **right**, the accounting information is stored at the home server 51 side, and the usage **right** is delivered to the stationary apparatus 52.

FIG. 75 is a flow chart showing processing where the home server 51 changes the content usage **right** that has been already purchased to another usage pattern and purchases it. Step S240 to Step S245 of FIG. 75 are processes similar to those... ...cipher processing portion 65 of the home server 51 makes the external memory controlling portion 97 of the cipher processing portion 65 read out the **license** condition information of the contents of which usage **right** is changed. Read-out of data from the external memory 67 has been described referring to FIG. 68, and detailed description thereof is thus omitted. In the case where the **license** condition information can be normally read out in Step S246, advancement to Step S247 is made.

In Step S247, the host controller 62 of the home server 51 displays information of contents of which usage **right** content can be changed (for example, usage patterns and prices of which usage **right** content can be changed) using the displaying means 64, and user selects usage **right** contents update condition using the inputting means 63. A signal inputted from the inputting means 63 is sent to the host controller 62 of the home server 51, and the host controller 62 generates a usage **right** contents changing demand based on the signal and inputs the usage **right** contents changing demand in the cipher processing portion 65 of the home server 51. The cipher processing portion 65, which receives this, generates accounting information and new **license** condition information from the handling policy received in Step S243, the price information received in Step S245 and the **license** condition information read out in Step S247.

Step S248 is similar to Step S171 of FIG. 67, and detailed description thereof is thus omitted. In Step S249, the controlling portion 91 of the cipher processing portion 65

outputs the **license** condition information generated in Step S247 to the external memory controlling portion 97 of the cipher processing portion 65. The external memory controlling portion 97 rewrites and updates in the external memory 67 the received **license** condition information. A method for rewriting (updating) in the external memory 67 of the external memory controlling portion 97 has been described with reference to FIG. 70, and detailed description thereof is thus omitted.

In Step S246, if **license** condition information corresponding to the content ID added to the **right** contents changing command is not found in the external memory 67, or if a tamper is found in the memory block of the external memory in which the **license** condition information is stored (already described referring to FIG. 68), advancement to Step S251 is made, and predetermined error processing is performed.

In this way, the home server 51 may purchase new **right** using the **right** that has been already purchased, and the handling policy and price information to change usage **right** contents.

FIG. 76 and FIG. 77 show specific examples of the rule component of the handling policy and price information. In FIG. 76, the handling policy is constituted by a rule number added as a reference number for each usage **right**, a usage **right** content number indicating the usage **right** contents, its parameter, a minimum selling price and the rate of benefits of the content provider, and in this handling policy are described five rules, for example. For the rule 1, since the **right** item is of usage **right** content number 1, it is understood from FIG. 44 that the **right** is playback **right** and **right** with no limit on time and the number of times. Also, it is understood that there is no particular description in the parameter item. The minimum-selling price is (Yen)350. The earnings of the content provider 2 are 30% of the price. For the rule 2, since the **right** item is of usage **right** content number 2, it is understood from FIG. 44 that the **right** is playback **right** and **right** with limit on time and no limit on the number of times. Also, it is understood from the parameter item that the period limited for... ...minimum-selling price is (Yen)100, and the earnings of the content provider 2 is 30% of the price. For the rule 3, since the **right** item is of usage **right** content number 6, it is understood from FIG. 44 that the **right** is replication **right** (with no copy control signal), and **right** with no limit on time and with limit on the number of times. Also, it is understood from the parameter item that the number of... ...minimum-selling price is (Yen)30, and the earnings of the content provider 2 are 30% of the price.

For the rule 4, since the **right** item is of usage **right** content number 13, it is understood from FIG. 44 that the **right** is change of usage contents. It is understood from the parameter item that changeable rule numbers are from #2 (playback **right**, with limit on time and no limit on the number of times) to #1 (playback **right** wit no limit on time and the number of times) . The minimum-selling price is (Yen)200, and the earnings of the content provider 2 are 20% of the price. The minimum-selling price presented is lower that that of the rule 1 because it is intended that the **right** already purchased is taken as a trade-in and repurchased, and the earnings of the content provider 2, which are presented, are lower than those of the rule 1 for the purpose of increasing the earnings of the

electronic distribution service center 1 that is involved in practical works (Because the content provider 2 has no works when the **right** contents are changed).

For the rule 5, since the **right** item is of usage **right** content number 14, it is understood from FIG. 44 that the **right** is redistribution. It is understood from the parameter item that the redistribution enabling condition is that the apparatus having the rule number #1 (playback **right** with no limit on time and the number of times) purchases and redistributes the rule number 1 (playback **right** with no limit on time and the number of times) . The minimum-selling price is (Yen)250, and the earnings of the content provider 2 are 20% of the price. The minimum-selling price presented is lower than that of the rule 1 because the apparatus having **right** already purchased intends to repurchase the **right** for the same contents, and the earnings of the content provider 2, which are presented, are lower than those of the rule 1 for the purpose of increasing the earnings of the **electronic** distribution service center 1 that is involved in practical works (Because the content provider 2 has no works during redistribution).

In FIG. 77, price information is constituted by a rule number added as a reference number for each usage **right**, a parameter and price information, and in this price information are also described five rules. The rule 1 is price information for the rule #1 of the handling policy, and shows that the price is (Yen)500 and the earnings of the service provider 3 are 30% when the usage **right** content number #1 is purchased. Thus, of (Yen)500 paid by the user, the content provider 2 will take (Yen)150, the service provider 3 (Yen)150, and the **electronic** distribution service center 1 (Yen)200. The rules 2 to 5 are in a similar way, and detailed description thereof is thus omitted.

Furthermore, in... ...1 because the user apparatus perform distribution operations of the service provider 2 as a proxy, and collection of paid money is performed by the **electronic** distribution service center 1.

Also, in this example, rule numbers are consecutive numbers from #1 to #5, but the numbers are not necessarily consecutive. The creator defines a usage **right** number and a parameter for each rule number and arranges those extracted therefrom, which does not result in consecutive numbers in general.

FIG. 78 shows a specific example in the case of performing change of **right** contents described with reference to FIG. 75. The handling policy is constituted by a rule number added as a reference number for each usage **right**, a usage content number indicating the usage **right** contents, its parameter, a minimum-selling price and the rate of benefits of the content provider, the price information is constituted by a rule number added as a reference number for each usage **right**, a parameter and a price information and the **license** condition information is constituted by a rule number added as a reference number for each usage **right**, a usage **right** content number indicating the usage **right** content and its parameter. The home server 51 has already purchased playback **right** of rule number #2, **right** with limit on time, the rule number #2 is described in the **license** condition information indicating the **right** contents, and usage possible time is remaining thirty minutes, indicating that total two hours's purchase has been made up to the present

time. If a change from **right** with limit on time to **right** no limit on time is to be made, now, it is understood, from the rule 3 of the handling policy, the rule 3 of the price information and the **license** condition information, that a change to playback **right** with no limit on time and the number of times can be made with (Yen)200, and the **license** condition information changes to the role number #1, playback **right** of the usage **right** content number, with no limit on time and the number of times (The parameter in the case of usage **right** content number #1 will be described later. Also, as for this example, **right** with limit on time is once purchased, and then its **right** contents are changed, resulting in lower costs compared to cases where playback **right** with no limit on time and the number of times is directly purchased. Therefore, it is advisable to see total usage time to give a discount) .

FIG. 79 is a flow chart explaining a detailed process in which home server 51 purchases content usage **right** for the stationary apparatus 52, and redistributes the usage **right**. Step S260 to Step S264 are similar to Step S220 to Step S225 of FIG. 74, and detailed description thereof is thus omitted. In Step... ...of the home server 51 makes the external memory controlling portion 97 of the cipher processing portion 65 read from the external memory 67 the **license** condition information corresponding to the contents to be **redistributed** and the **content** key Kco)) encrypted with the save key Ksave)). A method of reading from the external memory 67 by the external controlling portion 97 has been... ...command in the cipher processing portion 65 of the home server 51. The cipher processing portion 65, which receives this, generates accounting information and new **license** condition information from the handling policy and the price information received in Step S264 and the **license** condition information read out in Step S265.

Step S267 is similar to Step S171 of FIG. 67, and detailed description thereof is thus omitted. In... ...during cross authentication in Step S260. Finally, the signature generation unit 114 of the encryption/decryption module 96 generates the signature corresponding to the new **license** condition information generated in Step S266, and sends the signature to the controlling portion 91 of the cipher processing portion 65.

Processes of Step S269... ...Step S232, and detailed description thereof is thus omitted.

In this way, the home server 51 can perform redistribution of the contents, by creating new **license** condition information from the usage **right** (**license** condition information) retained on its own and the handling policy and price information, and sending the new **license** condition information to the stationary apparatus 52 together with the content key Kco)) and the contents retained on its own.

FIG. 80 is a flow chart explaining a detailed process in which the home server 51 sends **license** condition information and the content key Kco)) for the stationary apparatus 52 to purchase content usage **right** by the stationary apparatus 52. In step S280, the cipher processing portion 73 of the stationary apparatus 52 determines whether or not a total charge... ...controlling portion 91 of the cipher processing portion 65 generates the signature for the content key Kco)) encrypted with the temporary key Ktemp)) and the **license** condition information read out in Step S284, using the signature generation unit

114 of the encryption/decryption module 96, and sends the signature to the host controller 62. The host controller 62 of the home server 51, which receives the content key Kco)) encrypted with the temporary key Ktemp)), the **license** condition information and signatures thereof, reads the contents encrypted with the content key Kco)), and the handling policy and the signature thereof, and price information... ...from the large capacity storing portion 68, and sends to the stationary apparatus 52 the content key Kco)) encrypted with the temporary key Ktemp)), the **license** condition information, signatures thereof, the contents encrypted with the content key Kco)), the handling policy and the signature thereof, and the price information and the... ...command in the cipher processing portion 73 of the stationary apparatus 52. The cipher processing portion 73, which receives this, generates accounting information and new **license** condition information from the handling policy, price information and the **license** condition information read out in Step S286.

In Step S290, the cipher processing portion 73 of the stationary apparatus 52 stores the accounting information generated... ...memory module (not shown) of the cipher processing portion 73.

In Step S292, the cipher processing portion 73 of the stationary apparatus 52 sends the **license** condition information generated in Step S289 and the content key Kco)) encrypted with the save key Ksave)) 2, generated in Step S291, to external memory controlling portion (not shown) of the cipher processing portion 73. The external memory controlling portion, which receives **license** condition information and the content key Kco)) encrypted with the save key Ksave)) 2, writes in the external memory 79 the **license** condition information and the content key Kco)) encrypted with the save key Ksave)) 2. A tamper check when write is performed has been described using FIG. 69, and detailed description thereof is thus omitted.

In this way, the stationary apparatus 52 receives from the home server 51 the usage **right** (**license** condition information), the handling policy, price information, the content key Kco)) and the contents which are retained by the home server 51, and creates new **license** condition information, thereby being able to receive redistribution of the contents.

FIG. 81 explains management transfer **right**. Management transfer is an operation by which playback **right** can be transferred from an apparatus 1 to an apparatus 2, and the transfer is same as a usual transfer in that **right** is transferred from the apparatus 1 to the apparatus 2, but is different from a usual transfer in that the apparatus 2 cannot retransfer the received playback **right** (The apparatus 1, after transfer of playback **right**, cannot retransfer the playback light, as in the case of a usual transfer) . The apparatus 2, which receives the playback **right** through management transfer, can give the playback **right** back to the apparatus 1, and after it is given back, the apparatus 1 can transfer the playback **right** again, but the apparatus 2 is still unable to do so. For achieving those, purchasers of management transfer **right** and current owners of management transfer **right** are managed with **license** condition information (Although it is assumed here that management transfer is possible only when having the usage **right** content number #1, it may be extended for the usage **right** content number #2).

In FIG. 81, the rule 1 of the handling policy has been described with reference to FIG. 78, detailed description thereof is thus omitted. For the rule 2, since the **right** item is of usage **right** content number 16, it is understood from FIG. 44 that the **right** is management transfer **right**. Also, it is understood that there is no particular description in the parameter item. The minimum-selling price is (Yen)100, and the earnings of... ...of the handling policy, and shows that the price is (Yen)100 and the earnings of the service provider 3 is 0% when the usage **right** content number #16 ...purchased. Thus, of (Yen)100 paid by the user, the content provider 2 will take (Yen)50, the service provider 3 (Yen)0, and the **electronic** distribution service center 1 (Yen)50.

In FIG. 81, the user first purchases the rule number #1 (playback **right**, with no limit on time and the number of times). However, the user does not have management transfer **right** at this time (state of (a) of FIG. 81). Then, the user purchases management transfer **right** (Because these operations occur instantly, it seems as if the user purchased them together). For the rule number of **license** condition information, the ID of the cipher processing portion representing a purchaser (herein after referred to as a purchaser) is ID 1 (for example, the ID of the home server 51), and the ID of the cipher processing portion possessing playback **right** (hereinafter, referred to as a possessor) is ID 2 (state of (b) of FIG. 81). When this is transferred to the stationary apparatus 52 by performing management transfer, for the rule component of the **license** condition information possessed by the home server 51, the purchaser is still ID 1, but the possessor changes to ID 2. Also, the rule component of the **license** condition information possessed by the stationary apparatus 52 receiving playback **right** through management transfer, in which the purchaser is ID 1 and the possessor is ID 2, is same as the case of the **license** condition information of the home server 51.

FIG. 82 is a flow chart explaining detailed transfer processing of management transfer **right**. In FIG. 82, Step S300 is similar to Step S220 in FIG. 74, and detailed description thereof is thus omitted. Also, Step S301 is similar... ...description thereof is thus omitted. In Step S303, the cipher processing portion 65 of the home server 51 examines the rule component of the read **license** condition information, and determines whether the usage **right** is playback **right** with no limit on time and the number of times and with management transfer **right**. If it is determined that there is management transfer **right**, advancement to Step S304 is made.

In Step S304, the controlling portion 91 of the cipher processing portion 65 determines whether both the purchaser and the possessor of the management transfer **right** are the ID of the home server 51. If it is determined that the purchaser and the possessor of the management transfer **right** are the ID of the home server 51, advancement to Step S305 is made. In Step S305, the controlling portion 91 of the cipher processing portion 65 rewrites the possessor of the management transfer **right** of **license** condition information to the ID of the stationary apparatus 52. In Step S306, the controlling portion 91 of the cipher processing portion 65 outputs the **license** condition information rewritten in Step S305 to the external memory controlling portion 97 of the cipher processing portion 65. The external memory controlling portion 97 of the cipher processing portion 65, which receives the **license** condition information, overwrites the **license** condition information

and stores it in the external memory 67. A method for rewriting and storing data in the external memory 67 has been described... ...S307 to Step S311 are similar to Step S268 to Step S272 of FIG. 79, and detailed description thereof is thus omitted.

If management transfer **right** is not included in the **license** condition information in Step S303, and if the purchaser or the possessor of management transfer **right** is not the home server 51 in Step S304, processing is suspended.

In this way, the **right** to play back the contents can be transferred from the home server 51 to the stationary apparatus 52.

FIG. 83 is a flow chart explaining processing where management transfer **right** is given back to the home server 51 that is a purchaser of the management transfer **right** from the stationary apparatus 52 currently possessing the management transfer **right**. In FIG. 83, Step S320 is similar to Step S220 in FIG. 74, and detailed description thereof is thus omitted. Step S321 is similar to... ...description thereof is thus omitted, but it is assumed that the home server 51 and the stationary 52 mutually determine whether they have management transfer **right**. If it is determined that they have management transfer **right**, advancement to Step S324 is made.

In Step S324, the cipher processing portion 65 of the home server 51 determines whether the purchaser of management transfer **right** is the ID of the home server 51 and the possessor is the ID of the stationary apparatus 52. If it is determined that the purchaser of management transfer **right** is the ID of the home server 51 and the possessor is the ID of the stationary apparatus 52, advancement to Step S325 is made. In a similar way, the cipher processing portion 73 of the stationary apparatus 52 determines whether the purchaser of management transfer **right** is the ID of the home server 51 and the possessor is the ID of the stationary apparatus 52. If it is determined that the purchaser of management transfer **right** is the ID of the home server 51 and the possessor is the ID of the stationary apparatus 52, advancement to Step S325 is made... ...the cipher processing portion 73 delete the content key Kco)) encrypted with the save key Ksave)) 2 stored in the external memory 79 and the **license** condition information. A method of deletion in the external memory 79 has been described with reference to FIG. 71, and detailed description thereof is thus omitted.

In Step S327, the controlling portion 91 of the cipher processing portion 65 generates **license** condition information with the possessor of management transfer **right** of **license** condition information rewritten to the ID of the home server 51. In Step S328, the controlling portion 91 of the cipher processing portion 65 outputs the **license** condition information generated in Step S327 to the external memory controlling portion 97 of the cipher processing portion 65. The external memory controlling portion 97 of the cipher processing portion 65, which receives the **license** condition information, overwrites the **license** condition information and stores it in the external memory 67. A method of rewriting the **license** condition information and storing it in the external memory 67 has been described with reference to FIG. 70, and detailed description thereof is thus omitted... ...s apparatus ID is not registered in the home server 51 or the stationary

apparatus 52 in Step S321, and if the content key or **license** condition information for predetermined contents is not found, and the memory block including them are tampered in the home server 51 or the stationary apparatus 52 in Step S322, advancement to Step S329 is made to perform error handling.

If there is no management transfer **right** in the **license** condition information in the home server 51 or the stationary apparatus 52 in Step S323, and if the purchaser is not the home server 51 and the possessor is not stationary apparatus 52, processing is suspended.

In this way, the **right** to play back the contents can be given back to the home server 51 from the stationary apparatus 52.

Furthermore, only a single contents, content... ...processing by use of the individual key

The content provider 2 encrypts the contents with the content key created on its own as described in **terms** of FIG. 9. Also, the content provider 2 receives the individual key specific to the content provider and the individual key encrypted with the distribution key from the **electronic** distribution service center 1, and encrypts the content key with the individual key. Thus, the content provider 2 supplies the contents encrypted with the content... ...3.

At the user home network 5, the individual key specific to the content provider 2 is decrypted using the distribution key received from the **electronic** distribution service center 1. In this way, the user home network 5 can decrypt the content key encrypted with the individual key specific to the... ...conditions of the content key Kco)), and so on are described (for example, a handling policy generating portion 206 in FIG. 84), means for generating **digital** signatures for various kinds of data (for example, a signature generating portion 207 in FIG. 84), means for verifying signature data generated for various kinds...85).

(3) Remote playback process

A remote playback process in which a playback command is received by a apparatus that does not retain the playback **right** of the contents (for example, the stationary apparatus 52) from a apparatus that retains the contents (for example, the home server 51), and the contents... ...the cipher processing portion 65 of the home server 51 makes the external memory controlling portion 97 of the cipher processing portion 65 read the **license** condition information corresponding to the contents to be subjected to remote playback and the content key Kco)) encrypted with the save key Ksave)) from the... ...Step S 416, the host controller 72 inserts the data indicated from the cipher processing portion 73 into the contents in the form of the **electronic** watermark. In this connection, the data that are passed from the cipher processing portion 73 to the extending portion 74 include not only the content key Kco)) and the playback command, but also playback conditions (analogue output, **digital** output and output with copy control signals (SCMS)) and the ID

of the apparatus that has purchased content usage **right**. The data to be inserted is the ID of the apparatus that has purchased the content usage **right**, namely the apparatus ID in **license** condition information, and so force. In Step S417, the extending portion 74 plays back **music** through a speaker (not shown).

In the configuration described above, the home server 51 sends the contents, the playback command of the contents and the content key Kco)) to the stationary apparatus 52, whereby the stationary apparatus 52 retaining no content playback **right** can play back the contents using the playback command and the content key Kco)). Thus, according to the aforesaid configuration, a plurality of apparatuses (such as stationary apparatuses) connected to an apparatus retaining the contents (an apparatus having content playback **right**) can play back the contents.

(4) Booking purchase processing

Booking purchase processing in which the key of the contents is converted in advance before the...in the external memory 67. Since this booking purchase processing does not involve actual purchase of the contents, out of purchase processing described above in **terms** of FIG. 67, processing as to accounting information in registration information update determination processing of Step S161, processing as to purchased contents corresponding to Step... ...to Step S168, processing as to verification of the signature of the price information corresponding to Step S169, and processing of storing accounting information and **license** condition information corresponding to Step S170 to Step S172 are not necessarily performed.

In this connection, in the case of the booking purchase processing of FIG. 87, the home server 51 does not create **license** condition information, but it is also possible to create **license** condition information and define its usage **right** content number (namely, **right** item) as a state of not possessing **right**, such as an initial value (for example, nonexistence #0).

In this way, in the booking purchase processing, the home server 51 stores the content key... ...date of the distribution key Kd)) is reached, thereby making it possible perform purchase regardless of the expiration date of the distribution key Kd)) in **terms** of contents encrypted with the stored content key Kco)).

Now, processing of real purchase of the contents for which the booking of purchase has been...purchase command in the cipher processing portion 65 of the home server 51. The cipher processing portion 65, which receives this, generates accounting information and **license** condition information from the handling policy inputted in Step S475 and the price information inputted in Step S477. Accounting information is same as that described... ...module 92 the accounting information generated in Step S478. And in Step S480, the controlling portion 91 of the cipher processing portion 65 sends the **license** condition information generated in Step S478 to the external memory controlling portion

97 of the cipher processing portion 65. The external memory controlling portion 97, which receives the **license** condition information, makes a tamper check for the external memory 67, followed by writing the **license** condition information in the external memory 67. A tamper check when the **license** condition information is written is same as that described above with reference to FIG. 69, and detailed description thereof is thus omitted (Furthermore, in the case where **license** condition information with no **right** is already written, the **license** condition information is rewritten and updated by means of rewrite processing described with reference to FIG. 70).

In this connection, if it is determined in... ...proceeds to Step S481 to perform error handling.

As described above, the home server 51 stores in the memory module 92 the accounting information in **terms** of the content selected for purchase by the user, and stores the **license** condition information in the external memory 67, thereby ending real purchasing processing of the contents. In this real purchase processing, verification of the signature of... ...from each other in registration information (Registration List), namely apparatuses different from each other in groups will be described. In this proxy purchase processing, in **terms** of cases where the contents are exchanged between the home server 51 and portable devices and the like, which are non-group apparatuses as opposed...controlling portion 91 of the cipher processing portion 65 generates the signature for the content key Kco)) encrypted with the temporary key Ktemp)) and the **license** condition information generated in Step S509, using the signature generation unit 114 of the encryption/decryption module 96, and sends the signature to the host controller 62. The host controller 62 of the home server 51, which receives the content key Kco)) encrypted with the temporary key Ktemp)), the **license** condition information and their signatures, reads the contents encrypted with the content key Kco)) from the large capacity storing portion 68, and sends the content key Kc)), encrypted with the temporary key Ktemp)), the **license** condition information, their signatures and the contents encrypted with the content key Kco)) to the non-group apparatus.

In Step S513, the non-group apparatus, which receives the content key Kco)) encrypted with the temporary key Ktemp)), the **license** condition information, their signatures and the contents encrypted with the content key Kco)), outputs the contents encrypted with the content key Kco)) to the recording... ...S515, the cipher processing portion 73 of the non-group apparatus sends the content key Kco)) encrypted with the save key Ksave)) 2 and the **license** condition information received in Step S513 to the external memory controlling portion of the cipher processing portion 73, and has them stored in the external... ...has been described with reference to FIG. 69, and detailed description thereof is thus omitted.

In this way, the home server 51 purchases content usage **right**, accounting information is stored by the home server 51, and the usage **right** is passed to the non-group apparatus. By this, the home server 51 pays for the content usage **right** passed to the non-group apparatus.

Then, FIG. 90 shows a processing procedure where the home server 51 passes the contents to the non-group...the signal, and inputs the purchase command in the cipher processing portion 73. The cipher processing portion 73, which receives this, generates accounting information and **license** condition information from the handling policy and the price information inputted in Step S560. The accounting information has been described with reference to FIG. 42, and detailed description thereof is thus omitted. The **license** condition information has been described with reference to FIG. 41, and detailed description thereof is thus omitted.

In Step S562, the cipher processing portion 73... ...2 is stored in the external memory 79 from the cipher processing portion 73.

In this way, the home server 51 passes the content usage **right** already purchased to the non-group apparatus, and the non-group apparatus stores the accounting information, whereby the non-group apparatus pays for the content usage **right** passed from the home server 51 outside the group.

In the configuration described above, as described with reference to Step S502 and Step S554, registration... ...contents possessed by one apparatus can be passed to the other apparatus after it is confirmed that they are registered apparatuses, as described above in **terms** of aforesaid Step S502 to Step S554. Thus, according to the aforesaid configuration, contents can be exchanged between apparatuses different from each other in groups... ...or price information is included description about whether or not verification is needed, and operations are performed in accordance therewith.

(6) Another configuration of the **electronic music** distribution system

FIG. 91 explains another configuration of an **electronic music** distribution system 400. In such an **electronic music** distribution system 400, to an **electronic** distribution service center 401 of personal computer configuration are connected personal computers 403 and 406 for signal processing (hereinafter referred to as signal processing personal... ...communication terminal (a portable information device, a cellular phone and the like) are connected to the home server 409.

As shown in FIG. 92, the **electronic** distribution service center 401 has a configuration in which a RAM (Random Access Memory) 417, a ROM (Read Only Memory) 418, a displaying portion 419...cross authenticating portion 17, the user managing portion 18, the account charging portion 19, the banking portion 20 and the auditing portion 21 of the **electronic** distribution service center 1 as described above with reference to FIG. 2, in accordance with various kinds of these programs.

Also, the controlling portion 415... ...records of contents with the content provider 404, the service provider 407, the user home network 408, JASRAC and the like.

In this way, the **electronic** distribution service center 401 of personal computer configuration can achieve functions similar to those of the **electronic** distribution service center 1 described above with reference to FIG. 2 in accordance with various kinds of programs.

In this connection, in the **electronic** distribution service center 401, use of the inputting portion 420 and the displaying portion 419 may be prevented and thus the inputting portion 420 and... ...displaying portion 419 may be used for confirming various kinds of information recorded in the hard disk drive 421 and so on.

Also, in the **electronic** distribution service center 401, various kinds of programs may be recorded in advance in the hard disk of the hard disk drive 421 in place... ...437, a ROM 438, a displaying portion 439, an inputting portion 440, a hard disk drive 441, a network interface 442 for connection to the **electronic** distribution service center 401 and the service provider 407, and an IEEE 1394 interface 444 that is connected via the IEEE 1394 interface 432 and... ...advance in the ROM 438 to develop them on the RAM 437, the controlling portion 435 can perform processing as in the case of the **electronic** watermark adding portion 32, the compressing portion 33, the content encrypting portion 34, the content key generating portion 35, the content key encrypting portion 36...the distribution key Kd)), the individual key K1)) encrypted with the distribution key Kd)), the handling policy and the content provider secure container with the **electronic** distribution service center 401 and the service provider 407 via the network interface 442.

In this way, the content provider 404 of personal computer configuration... ...456, a ROM 457, a displaying portion 458, an inputting portion 449, a hard disk drive 460, a network interface 461 for connection to the **electronic** distribution service center 401 and the content provider 404, an IEEE 1394 interface 463 that is connected to the IEEE 1394 interface 452 of the...of these programs.

By this, the signal processing personal computer 406 can exchange price information, the content provider secure container and the like with the **electronic** distribution service center 401 and the content provider 407 via the network interface 442, and can send the service provider secure container to the user... ...interface 472, a modem 473 for connection to the service provider 407 via the network 4, and a network interface 474 for connection to the **electronic** distribution service center 401 are connected to a controlling portion 465 such as the CPU via a bus 466.

Also, in the user home network... ...network interface 474 may be integrated into one interface such as a modem, depending on patterns of communication with the service provider 407 and the **electronic** distribution service center 401. Furthermore, in the home server 409, the stationary apparatus 410 and the portable device 411 may be cable-connected via a...programs.

In this connection, in the portable device 411, a detachable medium may be provided for the recording and playing of the contents.

For the **electronic music** distribution system 400, in the aforesaid configuration, the **electronic** distribution service center 401, the content provider 404, the service provider 407 and the home server 409 of the user home network 408 are of personal computer configuration, respectively.

Thus, in the **electronic music** distribution system 400, the **electronic** service center 401, the content provider 404, the service provider 407 and the home server 409 do not need to be newly produced in hardware... ...installed in an existing personal computer, whereby a system can be easily constructed using such a personal computer.

According to the above described configuration, the **electronic music** distribution system 400 is constructed using the **electronic** distribution service center 401 of the personal computer configuration, the content provider 404, the service provider 407 and the home server 409, whereby an existing personal computer can be easily set as the **electronic** distribution service center 401, the content provider 404, the service provider 407 and the home server 409, thus making it possible to ease and simplify system construction.

Furthermore, for the **electronic music** distribution system 400, cases where the **electronic** distribution service center 401, the content provider 404, the service provider 407, the home server 409, the stationary apparatus 410 and the portable device 411... ...468, 478 and 493 have been described, but a program storing medium in which various kinds of programs are stored may be installed in the **electronic** distribution service center 401, the content provider 404, the service provider 407, the home server 409, the stationary apparatus 410 and the portable device 411, thereby operating respectively the **electronic** distribution service center 401, the content provider 404, the service provider 407, the home server 409, the stationary apparatus 410 and the portable device 411... ...programs transferred from the program storing medium to the hard disk and the like.

In this connection, the program storing medium used for operating the **electronic** distribution service center 401, the content provider 404, the service provider 407, the home server 409, the stationary apparatus 410 and the portable device 411...or permanently stored. Also, for means for storing programs in these program storing media, cable and wireless communication media such as local area networks, the **Internet** and **digital** satellite broadcasts may be used, and programs may be stored through various kinds of communication interfaces such as routers and modems.

INDUSTRIAL APPLICABILITY

The present invention may be used for information sending devices such as providers providing contents such as **music**, images and game programs, and information receiving devices such as personal computers and cellular phones receiving the provided contents, and further network systems constructed of...

Claims: ...key from an information sending device to an information receiving device: characterized in that said information receiving device comprises:

receiving end controlling means having usage **right** of said content data, and said content key for decrypting said content data distributed from said information sending device, and generating a playback command for another apparatuses that does not have the usage **right** of said content data; and

sending means for sending said playback command and said content key to said another apparatus, thereby having said content played... ...device to an information receiving device, characterized by comprising:

a generating step of generating a playback command for another apparatus that does not have usage **right** of said content data, by said information receiving device having usage **right** of said content data, and said content key for decrypting said content data distributed from said information sending device; and

a sending step of sending...key for decrypting said content data distributed from said information sending device, and generating a playback command for another apparatus that does not have usage **right** of said content data, if having usage **right** of said content data, and

sending means for sending said playback command and said content key to said another apparatus.

125.The information receiving device... ...information sending device, characterized by comprising:

receiving means for receiving a playback command and said content key sent from said information receiving device having usage **right** of said content data and said content key for decrypting said content data distributed from said information sending device, and receiving said content data sent from said information receiving device, if not having usage **right** of said content data; and

apparatus side controlling means for playing back said content data using said playback command and said content key.

129.The... ...method of an information receiving device, characterized by comprising:

a generating step of generating a playback command for another apparatus that does not have usage **right** of said content data, if having usage **right** of said content data, and said content key for decrypting said content data distributed from said information sending device; and

a sending step of sending... ...sending device, characterized by comprising:

a receiving step of receiving a playback command and said content key sent from said information receiving device having usage **right** of said content data, and said content key for decrypting said content data distributed from said information sending device, and receiving said content data sent from said information receiving device, if not having usage **right** of said content data; and

a playing step of playing back said content data using said playback command and said content key.

137.The playback...are used.

140.A program storing medium for making an information receiving device run a program, characterized by comprising:

a generating step if having usage **right** of a predetermined content data, and a predetermined content key for decrypting said content data that is encrypted with said content key and is distributed from an information sending device, generating a playback command for another apparatus that does not have usage **right** of said content data; and

a sending step of sending said playback command and said content key to said another apparatus.

141.The program storing... ...a program, characterized by comprising:

a receiving step of receiving a playback command and said content key sent from said information receiving device having usage **right** of said content data, and said content key for decrypting said content data distributed from said information sending device, and receiving said content data sent from said information receiving device if not having usage **right** of said content data; and .

a playing step of playing back said content data using said playback command and said content key,

145.The program...content data distributed from an information sending device by first and second information receiving devices, characterized in that

said first information receiving device having usage **right** of said content data comprises:

first sending means for sending first registration information of said first information receiving device to said second information receiving device... ...second information receiving devices mutually determine by said first and second controlling means whether or not said content data can be used, and said usage **right** is sent and passed from said first sending means of said first information receiving device to said second information receiving device if said first and... ...determining whether or not said content data can be used among a plurality of said information receiving devices; and

a passing step of passing usage **right** to a second information receiving device for which a first information receiving device having said usage **right** of said content data in a plurality of said information receiving devices determines that said content data can be used, thereby making it possible to use said content data by said second information receiving device to which said usage **right** is passed.

175. The content using method according to Claim 174, characterized in that

said first information receiving device having usage **right** of said content data comprises a retaining step of generating and retaining accounting information for used part of said content data that is used by said second information receiving device for which it is determined that said content data can be **used**.

176. The **content** using method according to Claim 174, characterized in that

said second information receiving device that receives usage **right** of said content data comprises a retaining step of generating and retaining accounting information for used part of said content data.

177. An information receiving...and second registration information whether or not said content data can be used, mutually with said other information receiving devices,

in which if having usage **right** of said content data, said controlling means passes said usage **right** through said sending means to said other information receiving devices for which it is determined that said content data can be used, thereby making it possible to use said content data by said other information receiving devices to which said usage **right** is passed.

178. The information receiving device according to Claim 177, characterized in that

said controlling means generates and retains accounting information for used part of said content. data that is used by said other information receiving devices to which usage **right** of said content data is passed.

179. The information receiving device according to Claim 178, characterized in that

        said controlling means retains said content data... ...on said handling
        policy data and said price information.

180. The information receiving device according to Claim 179, characterized in that

said controlling means generates **license** condition information describing usage **right** of said content data based on said handling policy data and said price information, and

said sending means sends said **license** condition information to said other information receiving devices as usage **right** of said content data.

181. The information receiving device according to Claim 180, characterized in that

said controlling means encrypts said content key with a... ...content data encrypted with said content key and said content key encrypted with said temporary key to said other information receiving devices together with said **license** condition information.

182. The information receiving device according to Claim 177, characterized in that

said controlling means retains said content data encrypted with a predetermined... ...said content key, and price information of said content data, and

said sending means sends said handling policy data and said price information for generating **license** condition information describing usage **right** of said content data and accounting information for used part of said content data to said other information receiving devices.

183. The information receiving device... ...second registration information whether or not said content data con be used, mutually with said other information receiving devices,

in which if not having usage **right** of said content data , said usage **right** sent from an information receiving device having usage **right** of said content data, in said other information receiving devices for which it is determined that said content data can be used, is received by... ...policy of a predetermined content key encrypting said content data, and price information of said content data, sent from an information receiving device having usage **right** of said content data, and

said controlling means generates and retains said accounting information based on said handling policy data and said price information.

187.The information receiving device according to Claim 186, characterized in that

said controlling means generates and retains **license** condition information describing usage **right** of said content data based on said handling policy data and said price information.

188.The information receiving device according to Claim 187, characterized in... ...key, and said content key encrypted with a temporary key shared with said other information receiving devices, sent from an information receiving device having usage **right** of said content data, and

said sending means decrypts said content key with said temporary key, encrypts the said decrypted content key with its specific... ...said registration information whether or not said content data can be used, mutually with other information receiving devices; and

a passing step of passing usage **right** to said other information receiving devices for which it is determined that said content data can be used, thereby making it possible to use said content data by said other information receiving devices to which said usage **right** is passed, if having said usage **right** of said content data.

190.The content using method according to Claim 189, characterized by comprising:

a generating and retaining step of generating and retaining accounting information for used part of said content data that is used by said other information receiving devices to which usage **right** of said content data is passed.

191.The content using method according to Claim 190, characterized in that

in said generating and retaining step, said... ...information of said content data, and is retained.

192.The content using method according to Claim 191, characterized in that

a generating step of generating **license** condition information describing usage **right** of said content data based on said handling policy data and said price information is comprised, and

in said passing step, said **license** condition information is passed to said other information receiving devices as usage **right** of said content data.

193.The content using method according to Claim 192, characterized in that

an encrypting step of encrypting said content key with... ...encrypted with said content key, and said content key encrypted with said temporary key is sent to said other information receiving devices together with said **license** condition information.

194.The content using method according to Claim 189, characterized in that

in said passing step, handling policy data describing handling policy of... ...data encrypted with the predetermined content key, and price information of said content data are passed to said other information receiving devices in order that **license** condition information describing usage **right** of said content data, and accounting information for used part of said content data are generated.

195.The content using method according to Claim 194... ...information whether or not said content data can be used, mutually with said other information receiving devices; and

a receiving step of receiving said usage **right** of said content data from an information receiving device having said usage **right** of said content data, in said other information receiving devices for which it is determined that said content data can be used, and making it possible to use said content data, if not having said usage **right** of said content data.

197.The content using method according to Claim 196, characterized by comprising:

a generating and retaining step of generating and retaining... ...policy of a predetermined content key encrypting said content data, and price information of said content data, sent from an information receiving device having usage **right** of said content data are received, and

in said generating and retaining step, said accounting information is generated based on said handling policy data and... ...price information and is retained.

199.The content using method according to Claim 198, characterized by comprising:

> an information generating step of generating and retaining **license** condition information describing usage **right** of said content data, based on said handling policy data and said price information.

200.The content using method according to Claim 187, characterized in... ...key, and said content key encrypted with a temporary key shared with said other information receiving devices, sent from an information receiving device having usage **right** of said content data, are received, and

a content retaining step of decrypting said content key with said temporary key, encrypting the decrypted content key... ...registration information whether or not said content data can be used, mutually with said other information receiving devices; and

a passing step of passing usage **right** of said content to said other information receiving devices for which it is determined that said content data can be used, thereby making it possible to use said content data by said other information receiving devices to which said usage **right** is passed, if having said usage **right** of said content data.

202.The program storing medium according to Claim 201, characterized by comprising:

> a generating and retaining step of generating and retaining accounting information for used part of said content data that is used by said other information receiving devices to which usage **right** of said content data is passed.

203.The program storing medium according to Claim 202, characterized in that

> in said generating and retaining step, said...information of said content data, and is retained.

204.The program storing medium according to Claim 203, characterized in that

a generating step of generating **license** condition information describing usage **right** of said content data based on said handling policy and said price information is comprised, and

in said passing step, said **license** condition information is passed to said other information receiving devices as usage **right** of said content data.

205.The program storing medium according to Claim 204, characterized in that

an encrypting step of encrypting said content key with... ...encrypted with said content key, and said content key encrypted with said temporary key are sent to said other information receiving devices together with said **license** condition information.

206.The program storing medium according to Claim 201, characterized in that

in said passing step, handling policy data describing handling policy of... ...data encrypted with the predetermined content key, and price information of said content data are passed to said other information receiving devices in order that **license** condition information describing usage **right** of said content data, and accounting information for used part of said content data are generated.

207.The program storing medium according to Claim 206... ...information whether or not said content data can be used, mutually with said other information receiving devices; and

a receiving step of receiving said usage **right** of said content data from an information receiving device having said usage **right** of said content data, in said other information receiving devices for which it is determined that said content data can be used, and making it possible to use said content data, if not having said usage **right** of said content data.

209.The program storing medium according to Claim 208, characterized by comprising:

a generating and retaining step of generating and retaining... ...policy of a predetermined content key encrypting said content data, and price information of said content data, sent from an information receiving device having usage **right** of said content data, are received, and

in said generating and retaining step, said accounting information is generated based on said handling policy data and said price information, and is retained.

211.The program storing medium according to Claim 210, characterized by comprising:

an information generating step of generating **license** condition information describing usage **right** of said content data based on said handling policy data and said price information, and retaining the same.

212.The program storing medium according to... ...key, and said content key encrypted with a temporary key shared with said other information receiving devices, sent from an information receiving device having usage **right** of said content data, are received, and

a content retaining step of decrypting said content key with said temporary key, encrypting the decrypted content key...

18/K/9 (Item 4 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

Country	Number	Kind	Date

Legal Status Type	Pub. Date	Kind	Text

Language

Fulltext Availability Available Text	Language	Update	Word Count
Total Word Count (Document A)			
Total Word Count (Document B)			
Total Word Count (All Documents)			

Specification: ...s) 109. This includes preview of sample Digital Content clips. Digital Content clips are not packaged into SC(s) but instead are integrated into the **web** service of the **Electronic Digital** Content Store(s) 103 as downloadable files or fed from a streaming server. The format of the Content 113 clip is not dictated by the system architecture. In another embodiment, the Player Application 195 could interact directly

with the **Electronic Digital** Content Store(s) 103 or Clearinghouse(s) 105 or offline using a promotional CD. B. Application Installation

The Player Application 195 and the Helper Application 1981 are packaged into a self installing executable program which is available for download from many **web** sites. The Clearinghouse(s) 105 acts as a central location which hosts the master download page at a public **web** site. It contains links to the locations from which the installation package can be downloaded. The installation package is available at all Content Hosting Site(s) 111 to provide geographic dispersal of the download requests. Each participating **Electronic Digital** Content Store(s) 103 can also make the package available for download from their site or may just provide a link to the master download page at the public **web** site of the Clearinghouse(s) 105.

Any End-User(s) wishing to purchase downloadable Content 113, downloads and install this package. The installation is self... ...package. It unpacks and installs both the Helper Application 198 and the Player Application 195 and also configure the Helper Application 198 to the installed **Web** Browser(s).

As part of the installation, a Public/Private Key 661 pair is created for the End-User Device(s) 109 for use in processing Order and **License** SC(s) 660. A random Symmetric Key (Secret User Key) is also generated for use in protecting song encryption keys in the **License** Database 197. The Secret User Key (not shown) is protected by breaking the key into multiple parts and storing pieces of the key in multiple... ...One product this code was introduced is in the IBM ThinkPad 770 laptop computer. Here, the tamper-resistant software was used to protect the DVD **movie** player in the computer. **Digital** Content Provider(s) such as Hollywood studios, concerned about the advent of **digital movies** and the ease at which perfect copies can be made, have insisted that **movies** on DVD disc(s) contain copy protection mechanisms. IBM's tamper-resistant software made it difficult to circumvent these copy protection mechanisms. This is a... ...hackers regarding its true operation. The latter technique is largely ad hoc, but the first two build upon well-known tools in cryptography: encryption and **digital** signatures.

C. Secure Container Processor 192

When the End-User(s) submits the final purchase authorization to the **Electronic Digital** Content Store(s) 103 for the merchandise he has collected in his shopping cart, his **Web** Browser remains active waiting for a response from the **Web** Server. The **Web** Server at the **Electronic Digital** Content Store(s) 103 processes the purchase and performs the financial settlement and then returns a Transaction SC(s) 640 to the End-User Device(s) 109. The SC(s) Processor 192 (Helper Application 198) is launched by the **Web** Browser to process the SC(s) mime type associated with the Transaction SC(s) 640. FIG. 14 is an example of user interface screens of... ...displayed with this information and the End-User(s) is presented with options to schedule the download(s) of the Content 113 (e.g. for **music**, songs or entire albums), step 1402. The End-User(s) can select immediate

download or can schedule the download to occur at a later time... ...at install time. This Order SC(s) 650 is sent via HTTP request to the Clearinghouse(s) 105. When the Clearinghouse(s) 105 returns the **License** SC(s) 660, the Helper Application 198 is re-invoked to process the **License** SC(s) 660. The **License** SC(s) 660 is then opened and the URL of the Content Hosting Site(s) 111 is extracted from the referenced Order SC(s) 650. The **License** SC(s) 660 is then sent to the specified Content Hosting Site 111, via http request through the Browser, requesting download of the Content SCusing the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the **License** SC(s) 660, which itself is first decrypted using the Private Key. The decrypted buffer is then passed to the watermarking function.

The watermarking 193 extracts the watermarking instructions from the **License** SC(s) 660 and decrypt the instructions using the Private Key of the End-User(s). The watermarking data is then extracted from the **License** SC(s) 660 which includes transaction information such as the purchaser's name as registered with the **Electronic Digital** Content Store(s) 103 from which this Content 113 was purchased or derived from the credit card registration information if the **Electronic Digital** Content Store(s) 103 does not provide a registration function. Also included in the watermark is the purchase date and the Transaction ID 535 assigned by the **Electronic Digital** Content Store(s) 103 to reference the specific records logged for this transaction. The Store Usage Conditions 519 are also included to be used by... ...encrypt the Content 113 using a random Symmetric Key. Once the download and Decryption and Re-Encryption 194 process is complete, the encryption Key 623 **used** by the **Content** Provider(s) 101 to originally encrypt the Content 113 is now destroyed and the new SEAL key is itself encrypted using the Secret User Key created and hidden at installation time. This new encrypted Seal Key is now stored in the **License** Database 107.

Unlike source performed at the Content Provider(s) 101 and user watermarking performed at the End User Device(s) 109 may need to become an industry standard to be effective. These standards are still evolving. The technology is available to allow control information to be embedded in the **music** and updated a number of times. Until such time as the copy control standards are more stable, alternative methods of copy control have been provided in the Secure **Digital** Content **Electronic** Distribution System 100 so that it does not rely on the copy control watermark in order to provide **rights** management in the consumer device. Storage and p lay/record usage conditions security is implemented utilizing encrypted DC Library Collections 196 that are tied to... ...Environment. Software hooks are in place to support copy control watermarking when standards have been adopted. Support exists today for watermarking AAC and other encoded **audio** streams at a variety of compression levels but this technology is still somewhat immature at this time to be put to use as a sole... ...in the selection of the original content encryption algorithm. Thus use of widely accepted and proven industry standard algorithms can be used thus further enhancing **Digital** Content Industry acceptance of the Secure **Digital** Content **Electronic** Distribution System 100.

The second purpose of this Decryption and Re-Encryption 194 process is to remove the requirement that the original master encryption Key 623, **used** by the **Content**

Provider(s) 101 to encrypt this Content 113, be stored on every End-User Device(s) 109 which has **licensed** this Content 113. The encrypted master Key 623, as part of the **License** SC(s) 660, is only cached on the hard disk of the End-User Device(s) 109 for a very short time and is in... ...Encryption 194 phase has completed, greatly lessens the possibility of piracy from hackers.

Once the song has been re-encrypted, it is stored in the **Digital** Content Library 196. All metadata required for use by the Player Application 195, is extracted from the associated Offer SC(s) 641 and also stored in the **Digital** Content Library 196, step 1403. Any parts of the metadata which are encrypted, such as the song lyrics, are decrypted and re-encrypted in the same manner as described above for the other content. The same SEAL key used to encrypt the **Content** 113 is **used** for any associated metadata needing to be encrypted.

D. The Player Application 195

1. Overview

The Secure **Digital** Content **Electronic** Distribution Player Application 195 (referred to here as the Player Application 195) is analogous to both a CD, DVD or other **Digital** Content player and to a CD, DVD, or other **digital** content storage management system. At its simplest, it performs Content 113, such as playing songs or videos. At another level, it provides the End- User(s) a tool for managing his/her **Digital** Content Library 196. And just as importantly, it provides for editing and playing of collections of content, such as songs, (referred to here as Play... ...195 is assembled from a collection of components that may be individually selected and customized to the requirements of the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103. A generic version of the player is described, but customization is possible.

Referring now to FIG. 15 there is shown a... ...sets may be selected, based on the requirements of:

(the platform (Windows, Unix, or equivalent)

(communications protocols (network, cable, etc)

(Content Provider(s) 101 or **Electronic Digital** Content Store(s) 103

(Hardware (CD, DVD, etc)

(Clearinghouse(s) 105 technology and more.

The sections below detail the various component sets. The final section... ...no definitive layout of these components. One such layout is provided in the generic player. Based on requirements from Content Provider(s) 101 and/or **Electronic Digital** Content Store(s) and other requirements, alternate layouts are possible.

This set is grouped into subgroups, starting with the components used to present End-User Display 1510 and handle controls called End-User Controls 1511 used for such low-level functions as **audio** playback , and presentation of metadata. Next, the End-User Display Component 1510 is further divided by special function groupings (Play-list, **Digital** Content Library), and then object-container components used for grouping and placing of those lower-level components.

Within the component listings below, any reference to... ...to a CD or other recordable medium only applies to the case where the Player Application 195 has such functionality enabled. Also note that the **term** CD in that context is a generic one, that can also represent various other external recording devices, such as MiniDisc or DVD.

FIG. 16 is... ...performing the Content 113:

(Play/Stop button

(Play button

(Stop button

(Pause button

(Skip forward button

(Skip backward button

(Volume control

(Track position control/display

(**Audio** channel volume level display and more.

Controls for the displaying metadata associated with the Content 113

(Cover Picture button

(Cover Picture object

(Artist Picture button... ...include (corresponding screens of an End-User Interface are shown 1601 - 1605):

Play-list of display container

(Play-list Management button

(Play-list Management window

(**Digital** Content search button

(**Digital** Content search Definition object

(**Digital** Content search Submit button

(**Digital** Content search Results object

(Copy Selected Search Result Item To Play-list button

(Play-list object (editable)

(Play-list Save button

(Play-list Play button

(Play-list Pause button

(Play-list Restart button

(Create CD from Play-list button and more.

Display of **Digital** Content Library 196

(**Digital** content library button

(**Digital** content librarian window

(**Digital** content categories button

(**Digital** content categories object

(By-artist button

(By-genre button

(By-label button

(By-category button

(Delete button

(Add-to-Play-list button

(Copy to CD button

(Song List object

(Song List display container and more

Containers and Misc.

(Player window container

(**Audio** controls container

(Metadata controls container

(Metadata display container

(Toolbar container object

(Sample button

(Download button

(Purchase button

(Record button

(Player Name object

(Label/Provider/Store... ...The use of the Content 113 by the Player Applications 195 on End User Device(s) 109 is logged into a database such as the **License** Database 197. The tracking of each use of Content 113 by the Player Application 195 can be transmitted to one or more logging sites such as the Clearing House(s) 105 or Content Provider(s) 101 or **Electronic Digital** Content Store(s) 103 or any site designated and coupled to Transmission Infrastructures 107. This transmission can be scheduled at predetermined times to upload the... ...example, when duplicating or copying the Content 113 stored at the End User Device(s) 109, on to an external device such as DVD Disc, **digital** tape, flash memory, mini Disc or equivalent read/writeable removable media, the use is updates to the logging site. This may be a precondition to... ...many times the Content 113 was performed; if the Content 113 has been duplicated or copied to an authorized external device such as DVD Disc, **digital** tape or mini-Disc. In cases where there are multiple distinct users of a single Player Application 195 on the End User Device(s) 109... ...any one time and the results extrapolated. In this present embodiment, the actual

usage can be measures for the users logging back onto a designated **web** site such as the **Electronic Digital** Content Store(s) 103 or Content Provider(s) 101.

4. Decryption 1505, Decompression 1506 and Playback Components 1506

These components use the keys acquired by the Copy/Play Management components to unlock the **audio** data acquired from the Data Management and Library Access components, apply the appropriate decompression to prepare it for playback, and use system **audio** services to play it. In an alternate embodiment, the **audio** data acquired from the Data Management and Library Access components may be copied to removable media such as CDS, diskettes, tapes or MiniDisks.

5. Data... ...well as handle requests for information about the stored songs.

6. Inter-application Communication Components 1508

These components are used for coordination between the Secure **Digital** Content **Electronic** Distribution Player and other applications (e.g., Browser, helper-app and/or plug-in, etc) that may invoke the Player Application 195, or that the... ...this diagram are required for any player, but may be replaced by specialized versions depending on such things as form of encryption or scrambling being **used**, types of **audio** compression, access methods for the Content 113 library, and more.

Above the Player Object Manager 1501 are Variable Objects 1512, which are mostly derived from... ...the Player Application 195

The following embodiment is for an example where the Player Application 195 running on End-User Device(s) 109 is an **audio** player where Content 113 is **music**. It should be understood to those skilled in the art that other types of Content 113 can be supported by the Player Application 195. A typical **audio** enthusiast has a library of CDS holding songs. All of these are available within the Secure **Digital** Content **Electronic** Distribution System 100. The set of songs that have been purchased from **Electronic Digital** Content Store(s) 103 are stored within a **Digital** Content Library 196 on his or her system. The groupings of songs that are analogous to physical CDS are stored as Play-lists. In some cases a Play-list exactly emulates a CD (e.g., all tracks of a commercially available CD has been purchased from an **Electronic Digital** Content Store(s) 103 as an on-line version of the CD and is defined by a Play-list equivalent to that of the CD). But most Play-lists is put together by End-User(s) to group songs they have stored in the **Digital** Content Libraries on their systems. However for the purposes of the ensuing

discussions, an example of a custom made **music** CD is **used** when the **term** a Play- list is mentioned.

When the End-User(s) starts the Player Application 195 explicitly, rather than having it start up via invocation from the SC(s) Processor 192 Application, it pre-loads to the last Play-list that was accessed. If no Play-lists exist in the **Digital** Content Library 196, the Play-list editor is started automatically (unless the user has turned off this feature via a preference setting). See The Play... ...of an End-User Interface 1603):

When the End-User(s) has invoked the Play-list function, these are the available functions:

* Open Play-list

* **Digital** Content Librarian is invoked to display a list of stored Play-lists for selection. Also see **Digital** Content Librarian below for more info.

* Edit Play-list

* Invokes the Play-list Editor (see below), primed with the current Play-list if one has... ...for more info.

* Play-list Info

* Display information about the Play-list.

* Song Info

* Display information about the selected song within the Play-list.

* Visit **web** site

* Load **web** site associated with this Play-list into browser.

* Librarian

* Open the **Digital** Content Librarian window. Also see **Digital** Content Librarian below for more info.

The Play-list Editor (corresponding screen of an End-User Interface 1603):

When invoking the Play-list editor, these are the End-User(s)' options:

* View/Load/Delete Play-lists

* **Digital** Content Librarian is invoked to display a list of stored Play-lists for selection of one to load or delete. Also see **Digital** Content Librarian below for more info.

* Save Play-list

* Current version of Play-list is saved in the **Digital** Content Library 196.

* Delete Song

* Currently selected song is deleted from Play-list.

* Add Song

* **Digital** Content Librarian is invoked in song-search mode, for selection of song to add to the Play-list. Also see **Digital** Content Librarian below for more info.

* Set Song Information

* Display and allow changes to information about the selected song within the play-list. This information is stored within the Play-list, and does not alter information about the song stored within the **Digital** Content Library 196. These things can be changed:

* Displayed Song Title

* End-User(s) notes about the song

* Lead-in delay on playing the song... ...play once, restart when done, etc)

* End-User(s) notes about this Play-list

Librarian (corresponding screen of an End-User Interface 1601):

* Open the **Digital** Content Librarian window. Also see **Digital** Content Librarian below for more info.

Song Play

When a song has been prepared for play, either by invoking the Player Application 195 with the song as an argument or by selecting a song for play from a Play-list or within the **Digital** Content Librarian, these are the End-User(s)' options: (corresponding screen of an End-User Interface 1601):

* Play

* Pause

* Stop

* Skip Backward

* Skip Forward

* Adjust Volume

* Adjust Track Position

* View Lyrics

* View Credits

* View CD Cover

* View Artist Picture

* View Track Information

* View other metadata

* Visit **web** site

* Play-list

* Librarian and more.

Digital Content Librarian The **Digital** Content Librarian can be invoked implicitly when selecting songs or Play-lists (see above) or may be opened in its own window for management of... ...each over all purchase transaction from an End User Device(s) 109. In addition, an Item Number 1806 is a unique identifier generated by the **Electronic Digital** Content Store 103 for each for each piece or member or title that forms part of the transaction. Stated Item Number 1806 tracks each item...

18/K/10 (Item 5 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

Country	Number	Kind	Date

Legal Status Type	Pub. Date	Kind	Text

Language

Fulltext Availability	Available Text	Language	Update	Word Count
Total Word Count (Document A)				
Total Word Count (Document B)				
Total Word Count (All Documents)				

Specification: ...Distribution and Licensing Control

FIG. 6 is a block diagram illustrating an overview of the Content Distribution and Licensing Control as it applies to the **License** Control Layer of FIG. 5. The figure depicts the case in which the **Electronic Digital** Content Store(s) 103, End-User Device(s) 109 and the Clearinghouse(s) 105 are interconnected via the **Internet**, and unicast (point-to-point) transmission is used among those components. The communication between the Content Provider(s) 101 and the **Electronic Digital** Content Store(s) 103 could also be over the **Internet** or other network. It is assumed that the Content-purchase commercial transaction between the End-User Device(s) 109 and the **Electronic Digital** Content Store(s) 103 is based on standard **Internet Web** protocols. As part of the **Web**-based interaction, the End-User(s) makes the selection of the Content 113 to purchase, provides personal and financial information, and agrees to the conditions of purchase. The **Electronic Digital** Content Store(s) 103 could obtain payment authorisation from an acquirer institution using a protocol such as SET.

It is also assumed in FIG. 6 that the **Electronic Digital** Content Store(s) 103 has downloaded the End-User Player Application 195 to an End-User Device(s) 109 based on standard **Web** protocols. The architecture requires that the **Electronic Digital** Content Store(s) 103 assigns a unique application ID to the downloaded Player Application 195 and that the End-User Device(s) 109 stores it for later application **license** verification (see below).

The overall **licensing** flow starts at the Content Provider(s) 101. The Content Provider(s) 101 encrypts the Content 113 using an encryption symmetric key locally generated, and... ...Conditions 519 associated with the Content Usage Control Layer 505.

The Content Provider(s) 101 distributes the Metadata SC(s) 620 to one or more **Electronic Digital** Content Store(s) 103 (step 601) and the Content SC(s) 630 to one or more Content Hosting Sites (step 602). Each **Electronic Digital** Content Store(s) 103, in turn creates an Offer SC(s) 641. The Offer SC(s) 641 typically carries much of the same information as the Metadata SC(s) 620, including the **Digital** Signature 624 of the Content Provider(s) 101 and the Certificate (not shown of the Content Provider(s) 101. As mentioned above, the **Electronic Digital** Content Store(s) 103 can add to or narrow the Store Usage Conditions 519 (handled by the Control Usage Control Layer) initially defined by the Content Provider(s) 101. Optionally, the Content SC(s) 630 and/or the

Metadata SC(s) 620 is signed with a **Digital** Signature 624 of the Content Provider(s) 101.

After the completion of the Content-purchase transaction between the End-User Device(s) 109 and the **Electronic Digital** Content Store(s) 103 (step 603), the **Electronic Digital** Content Store(s) 103 creates and transfers to the End-User Device(s) 109 a Transaction SC(s) 640 (step 604). The Transaction SC(s... ...Transaction Data 642 is encrypted with the Public Key 621 of the Clearinghouse(s) 105. Optionally, the Transaction SC(s) 640 is signed with a **Digital** Signature 643 of the **Electronic Digital** Content Store(s) 103.

Upon reception of the Transaction SC(s) 640 (and the Offer SC(s) 641 included in it), the End-User Player Application 195 running on End-User Device(s) 109 solicits **license** authorisation from the Clearinghouse(s) 105 by means of an Order SC(s) 650 (step 605). The Order SC(s) 650 includes the encrypted Symmetric... ...and the encrypted Application ID 551 from the End-User Device(s) 109. In another embodiment, the Order SC(S) 650 is signed with a **Digital** Signature 652 of the End-User Device(s) 109.

Upon reception of the Order SC(s) 650 from the End-User Device(s) 109, the Clearinghouse(s) 105 verifies:

1. that the **Electronic Digital** Content Store(s) 103 has authorisation from the Secure **Digital** Content **Electronic** Distribution System 100 (exists in the Database 160 of the Clearinghouse(s) 105);

2. that the Order SC(s) 650 has not been altered;

3. that the Transaction Data 642 and Symmetric Key 623 are complete and authentic;

4. that the **electronic** Store Usage Conditions 519 purchased by the End-User Device(s) 109 are consistent with those Usage Conditions 517 set by the Content Provider(s) 101; and

5. that the Application ID 551 has a valid structure and that it was provided by an authorised **Electronic Digital** Content Store(s) 103.

If the verifications are successful, the Clearinghouse(s) 105 decrypts the Symmetric Key 623 and the Transaction Data 642 and builds and transfers the **License** SC(s) 660 to the End-User Device(s) 109 (Step 606). The **License** SC(s) 660 carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the Public Key 661 of the End-User Device(s) 109. If any verification is not successful, the Clearinghouse(s) 105 denies the **license** to the End-User Device(s) 109 and informs the End-User Device(s) 109. The Clearinghouse(s) 105 also immediately informs the **Electronic Digital** Content Store(s) 103 of this verification failure. In an alternate embodiment, the Clearinghouse(s) 105 signs the **License** SC(s) 660 with its **Digital** Signature 663.

After receiving the **License** SC(s) 660, the End-User Device(s) 109 decrypts the Symmetric Key 623 and the Transaction Data 642 previously received from the Clearinghouse(s... ...the Content 113 using the Symmetric Key 623 (Step 609), and passes the Content 113 and the Transaction Data 642 to the other layers for **license** watermarking, copy/play coding, scrambling, and further Content 113 processing as described previously for FIG. 5.

Finally, the Clearinghouse(s) 105 on a periodic basis transmits summary transaction reports to the Content Provider(s) 101 and the **Electronic Digital** Content Store(s) 103 for auditing and tracking purposes (Step 610).

V. SECURE CONTAINER STRUCTURE

A. General Structure

A Secure Container (SC) is a structure... ...together and another digest is computed from them and then encrypted using the private key of the entity creating the SC(s) to create a **digital** signature. Parties receiving the SC(s) can use the **digital** signature to verify all of the digests and thus validate the integrity and completeness of the SC(s) and all of its parts.

The following... ...records need to be included:

* SC(s) version

* SC(s) ID

* Type of SC(s) (e.g. Offer, Order, Transaction, Content, Metadata or promotional and **License**.)

* Publisher of the SC(s)

* Date that the SC(s) was created

* Expiration date of the SC(s)

* Clearinghouse(s) URL

* Description of the digest algorithm used for the included parts (default is MD-5)

* Description of the algorithm used for the **digital** signature encryption (default is RSA)

* **Digital** signature (encrypted digest of all of the concatenated digests of the included parts)

SC(s) may include more than one BOM. For example, an Offer SC(s) 641 consists of the original Metadata SC(s) 620 parts, including its BOM, as well as additional information added by the **Electronic Digital** Content Store(s) 103 and a new BOM. A record for the Metadata SC(s) 620 BOM is included in the Offer SC(s) 641... ...the Metadata SC(s) 620 have records in the new BOM that was created for the Offer SC(s) 641. Only parts added by the **Electronic Digital** Content Store(s) 103 and the Metadata SC(s) 620 BOM have records in the new BOM.

SC(s) may also include a Key Description... ...was used to encrypt the encrypted part.

If the SC(s) does not contain any encrypted parts, then there is no Key Description part.

B. **Rights** Management Language Syntax and Semantics

The **Rights** Management Language consists of parameters that can be assigned values to define restrictions on the use of the Content 113 by an End-User(s... ...the Content 113 is the Usage Conditions 517. Each Content Provider(s) 101 specifies the Usage Conditions 517 for each of its Content 113 items. **Electronic Digital** Content Store(s) 103 interpret the Usage Conditions 517 in Metadata SC(s) 620 and use the information to provide select options they wish to... ...the End-User Device(s) 109 requests authorisation for the Content 113 based on Store Usage Conditions 519. Before the Clearinghouse(s) 105 sends a **License** SC(s) 660 to the End-User(s), the Clearinghouse(s) 105 verifies that the Store Usage Conditions 519 being requested are in agreement with... ...were encoded into the Content 113 are enforced.

The following are examples of Store Usage Conditions 519 for an embodiment where the Content 113 is **music**:

* Song is recordable.

* Song can be played n number of times.

C. Overview of Secure Container Flow and Processing

Metadata SC(s) 620 are built by Content Provider(s) 101 and are **used** to define **Content** 113 items such as songs. The Content 113 itself is not included in these SC(s) because the size of the Content 113 is typically too large for **Electronic Digital** Content Store(s) 103 and End- User(s) to efficiently download the containers just for the purpose of accessing the descriptive metadata. Instead, the SC... ...the Content 113. The SC(s) also includes

metadata that provides descriptive information about the Content 113 and any other associated data, such as for **music**, the CD cover art and/or **digital audio** clips in the case of song Content 113.

Electronic Digital Content Store(s) 103 download the Metadata SC(s) 620, for which they are authorised, and build Offer SC(s) 641. In short, an Offer SC(s) 641 consists of some of the parts and the BOM from the Metadata SC(s) 620 along with additional information included by the **Electronic Digital** Content Store(s) 103. A new BOM for the Offer SC(s) 641 is created when the Offer SC(s) 641 is built. **Electronic Digital** Content Store(s) 103 also use the Metadata SC(s) 620 by extracting metadata information from them to build HTML pages on their **web** sites that present descriptions of Content 113 to End-User(s), usually so they can purchase the Content 113.

The information in the Offer SC(s) 641 that is added by the **Electronic Digital** Content Store(s) 103 is typically to narrow the selection of Usage Conditions 517 that are specified in the Metadata SC(s) 620 and promotional data such as a graphic image file of the store's logo and a URL to the store's **web** site. An Offer SC(s) 641 template in the Metadata SC(s) 620 indicates which information can be overridden by the **Electronic Digital** Content Store(s) 103 in the Offer SC(s) 641 and what, if any, additional information is required by the **Electronic Digital** Content Store(s) 103 and what parts are retained in the embedded Metadata SC(s) 620.

Offer SC(s) 641 are included in a Transaction SC(s) 640 when an End-User(s) decides to purchase Content 113 from an **Electronic Digital** Content Store(s) 103. The **Electronic Digital** Content Store(s) 103 builds a Transaction SC(s) 640 and includes Offer SC(s) 641 for each Content 113 item being purchased and transmits... ...Clearinghouse(s) 105 validates and processes Order SC(s) 650 to provide the End- User Device(s) 109 with everything that is required to a **License** Watermark 527 and access purchased Content 113. One of the functions of the Clearinghouse(s) 105 is to decrypt the Symmetric Keys 623 that are... ...the SC(s) and encrypts them again with the Public Key 661 of the End-User Device(s) 109. The Clearinghouse(s) 105 builds a **License** SC(s) 660 that includes the newly encrypted Symmetric Keys 623 and updated watermarking instructions and sends it to the End-User Device(s) 109... ...the Clearinghouse(s) 105 returns to the End-User Device(s) 109 an HTML page or equivalent reporting the failure of the authorisation process.

A **License** SC(s) 660 provides an End-User Device(s) 109 with everything that is needed to access a Content 113 item. The End-User Device... ...Content Provider(s) 101 and include encrypted Content 113 and metadata parts. The End-User Player Application 195 uses the Symmetric Keys 623 from the **License** SC(s) 660 to decrypt the Content 113, metadata, and watermarking instructions. The watermarking instructions are then affixed into the Content 113 and the Content... ...template), although the entire original BOM is propagated. This is done because the entire BOM is required by the Clearinghouse(s) 105 to verify the **digital** signature in the original SC(s).

The Key Description Part columns of the following table define the records that are included in the Key Description... ...was used to encrypt the Symmetric Key 623 when the Key Id/Enc Key column is an encrypted Symmetric Key 623.

The following describes the **terms** that are used in the above Metadata SC(s) table:

* (Content URL) - A parameter in a record in the Key Description part. This is a... ...use of the Content 113.

* SC(s) Templates - Parts that define templates that describe the required and optional information for building the Offer, Order, and **License** SC(s) 660.

* Watermarking Instructions - A part that contains the encrypted instructions and parameters for implementing watermarking in the Content 113. The watermarking instructions may be modified by the Clearinghouse(s) 105 and returned back to the End-User Device(s) 109 within the **License** SC(s) 660. There is a record in the Key Description part that defines the encryption algorithm that was used to encrypt the watermarking instructions... ...obtain the proper authorisation to access the Content 113.

* Digest Algorithm ID - An identifier of the algorithm used to compute the digests of the parts.

* **Digital** Signature Alg ID - An identifier of the algorithm used to encrypt the digest of the concatenated part digests. This encrypted value is the **digital** signature.

* **Digital** Signature - A digest of the concatenated part digests encrypted with the public key of the entity that created the SC(s).

* Output Part - The name... ...of the metadata parts, and BOM from the Metadata SC(s) 620 are also included in the Offer SC(s) 641.

The following describes the **terms** that are used in the above Offer SC(s) 641 that were not previously described for another SC(s):

* Metadata SC(s) BOM - The BOM... ...s) 641 BOM includes the digest of the Metadata SC(s) 620 BOM.

* Additional and Overridden Fields - Usage conditions information that was overridden by the **Electronic Digital** Content Store(s) 103. This information is validated by the Clearinghouse(s) 105, by means of the received SC(s) templates, to make sure that anything that the **Electronic Digital** Content Store(s) 103 overrides is within the scope of its authorisation.

* **Electronic Digital** Content Store(s) Certificate - A certificate provided to the **Electronic Digital** Content Store(s) 103 by the Clearinghouse(s) 105 and signed by the Clearinghouse(s) 105 using its private key. This certificate is used by the End-User

Player Application 195 to verify that the **Electronic Digital** Content Store(s) 103 is a valid distributor of Content 113. The End-User Player Application 195 and Clearinghouse(s) 105 can verify that the **Electronic Digital** Content Store(s) 103 is an authorised distributor by decrypting the certificate's signature with the Clearinghouse's 105 Public Key 621. The End-User... ...shows the parts that are included in the Transaction SC(s) 640 as well as its BOM and Key Description parts.

The following describes the **terms** that are used in the above Transaction SC(s) 640 that were not previously described for another SC(s):

* Transaction ID 535 - An ID assigned by the **Electronic Digital** Content Store(s) 103 to uniquely identify the transaction.

* End-User(s) ID - An identification of the End-User(s) obtained by the **Electronic Digital** Content Store(s) 103 at the time the End-User(s) makes the buying selection and provides the credit card information.

* End-User(s)' Public... ...is used by the Clearinghouse(s) 105 to re-encrypt the Symmetric Keys 623. The End-User(s)' Public Key 661 is transmitted to the **Electronic Digital** Content Store(s) 103 during the purchase transaction.

* Offer SC(s) - Offer SC(s) 641 for the Content 113 items that were purchased.

* Selections of displays in the **Internet** browser window upon receipt of the Transaction SC(s) 640 or during the interaction between the End-User Device(s) 109 and the Clearinghouse(s... ...SC(s) 640, the following steps may be performed to verify the integrity and authenticity of the SC(s):

1. Verify the integrity of the **Electronic Digital** Content Store(s) 103 certificate using the Public Key 621 of the Clearinghouse(s) 105. The Public Key 621 of the Clearinghouse(s) 105 was... ...s) 109 after it was received as part of the initialisation of the End-User Player Application 195 during its installation process.

2. Verify the **Digital** Signature 643 of the SC(s) using the public key from the **Electronic Digital** Content Store(s) 103 certificate.

3. Verify the hashes of the SC(s) parts.

4. Verify the integrity and authenticity of each Offer SC(s... ...any change so that the Clearinghouse(s) 105 can validate the integrity of the Metadata SC(s) 620 and its parts.

The following describes the **terms** that are used in the above Order SC(s) 650 that were not previously described for another SC(s):

* Transaction SC(s) BOM - The BOM... ...from the End-User(s) that is used to charge the purchase to a credit card or debit card. This information is required when the **Electronic**

Digital Content Store(s) 103 that created the Offer SC(s) 641 does not handle the customer billing, in which case the Clearinghouse(s) 105 may handle the billing.

H. **License** Secure Container 660 Format

The following table shows the parts that are included in the **License** SC(s) 660 as well as its BOM. As shown in the Key Description part, the Symmetric Keys 623 that are required for decrypting the... ...been re-encrypted by the Clearinghouse(s) 105 using the End-User(s)' Public Key 661. When the End-User Device(s) 109 receives the **License** SC(s) 660 it decrypts the Symmetric Keys 623 and use them to access the encrypted parts from the **License** SC(s) 660 and the Content SC(s) 630.

I. Content Secure Container Formal

The following table shows the parts that are included in the Content SC(s) 630 as well as the The following describes the **terms** that are used in the above **License** SC(s) 660 that were not previously described for another SC(s):

* EU Pub Key - An identifier that indicates that the End-User(s)' Public... ...time stamp (or both) in order to determine which list is the most recent.

I. Content Secure Container Format

The BOM

The following describes the **terms** used in the above Content SC(s) 630 that were not previously described for another SC(s):

* Encrypted Content - Content 113 that was encrypted by... ...There is no Key Description part included in the Content SC(s) 630 since the keys required to decrypt the encrypted parts are in the **License** SC(s) 660 that is built at the Clearinghouse(s) 105.

VI. SECURE CONTAINER PACKING AND UNPACKING

A. Overview

The SC(s) Packer is a... ...specified parts. The SC(s) Packer 151, 152, 153 variety of hardware platforms supporting Windows' program at the Content Provider(s) 101, Clearinghouse(s) 105, **Electronic Digital** Content Store(s) 103 and other sites requiring SC(s) Packing. A BOM and, if necessary, a Key Description part are created and included in... ...Description parts and to include parts in the SC(s). Encryption of parts and Symmetric Keys 623 as well as computing the digests and the **digital** signature is also be performed by the packer. Encryption and digest algorithms that are supported by the packer are included in the packer code or... ...processed. Bundling the parts into a single object is the last step that is performed when building a SC(s).

- Indication as to whether the **digital** signature is omitted from the BOM part. If this flag is not set, then the **digital** signature is computed **right** before the SC(s) is bundled into a single object.

In an alternate embodiment, the interface to the packer for building a SC(s) is... ...on a single line with a new line indicating the start of a new record. The BOM usually includes digests for each part and a **digital** signature that can be used to validate the authenticity and integrity of the SC(s).

The record types within a BOM are as follows:

IP... ...Description part.

W part(underscore)name (digest)

Specifies the watermarking instructions part.

C part(underscore)name (digest)

Specifies the certificate(s) used to validate the **digital** signature.

T part(underscore)name (digest)

Specifies the Usage Conditions part.

YF part name (digest)

Specifies the Template part for the Offer SC(s) 641... ...part(underscore)name (digest)

Specifies the Template part for the Order SC(s) 650.

YL part(underscore)name (digest)

Specifies the Template part for the **License** SC(s) 660.

ID part(underscore)name (digest)

Specifies the ID(s) of the Content 113 of the item(s) of Content 113 being referenced.

CH part(underscore)name (digest)

Specifies the Clearinghouse(s) 105 certificate part.

SP part(underscore)name (digest)

Specifies the **Electronic Digital** Content Store(s) 103 certificate part.

B part(underscore)name (digest)

Specifies a BOM part for another SC(s) that has its parts or a... ...D part(underscore)name (digest)

Specifies a data (or metadata) part.

S An S record is a signature record the is used to define the **digital** signature of the SC(s). The **digital** signature is specified as follows:

S key(underscore)identifier signature(underscore)string signature(underscore)algorithm

The S record contains the key(underscore)identifier to indicate the encryption key of the signature, the signature(underscore)string, which is the base64 encoding of the **digital** signature bitstring, and the signature algorithm that was used to encrypt the digest to create the **digital** signature.

C. Key Description Part

The Key Description part is created by the packer to provide information about encryption keys that are needed for decryption... ...Key 623 bit string that was used to encrypt the part.

VII. CLEARINGHOUSE(S) 105

A. Overview

The Clearinghouse(s) 105 is responsible for the **rights** management functions of the Secure **Digital** Content **Electronic** Distribution System 100. Clearinghouse(s) 105 functions include enablement of **Electronic Digital** Content Store(s) 103, verification of **rights** to Content 113, integrity and authenticity validation of the buying transaction and related information, distribution of Content encryption keys or Symmetric Keys 623 to End-User Device(s) 109, tracking the distribution of those keys, and reporting of transaction summaries to **Electronic Digital** Content Store(s) 103 and Content Provider(s) 101. Content encryption keys are used by End-User Device(s) 109 to unlock Content 113 for which they have obtained **rights**, typically by a purchase transaction from an authorised **Electronic Digital** Content Store(s) 103. Before a Content encryption key is sent to an End-User Device(s) 109, the Clearinghouse(s) 105 goes through a verification process to validate the authenticity of the entity that is selling the Content 113 and the **rights** that the End-User Device(s) 109 has to the Content 113. This is called the SC Analysis Tool 185. In some configurations the Clearinghouse(s) 105 may also handle the financial settlement of Content 113 purchases by co-locating a system at the Clearinghouse(s) 105 that performs the **Electronic Digital** Content Store(s) 103 functions of credit card authorisation and billing. The Clearinghouse(s) 105 uses OEM packages such as ICVerify and Taxware to handle the credit card processing and local sales taxes.

Electronic Digital Content Store(s) Embodiment

An **Electronic Digital** Content Store(s) 103 that wants to participate as a seller of Content 113 in the Secure **Digital** Content **Electronic** Distribution System 100 makes a request to one or more of the **Digital** Content Provider(s) 101 that provide Content 113 to the Secure **Digital** Content **Electronic** Distribution System 100. There is no definitive process for making the request so long as the two parties come to an agreement. After the **digital** content label such as a **Music** Label e.g. Sony, Time-Warner, etc. decides to allow the **Electronic Digital** Content Store(s) 103 to sell its Content 113, the Clearinghouse(s) 105 is contacted, usually via E-mail, with a request that the **Electronic Digital** Content Store(s) 103 be added to the Secure **Digital** Content **Electronic** Distribution System 100. The **digital** content label provides the name of the **Electronic Digital** Content Store(s) 103 and any other information that may be required for the Clearinghouse(s) 105 to create a **digital** certificate for the **Electronic Digital** Content Store(s) 103. The **digital** certificate is sent to the **digital** content label in a secure fashion, and then forwarded by the **digital** content label to the **Electronic Digital** Content Store(s) 103. The Clearinghouse(s) 105 maintains a database of **digital** certificates that it has assigned. Each certificate includes a version number, a unique serial number, the signing algorithm, the name of the issuer (e.g., the name of Clearinghouse(s) 105), a range of dates for which the certificate is considered to be valid, the name **Electronic Digital** Content Store(s) 103, the public key of the **Electronic Digital** Content Store(s) 103, and a hash code of all of the other information signed using the private key of the Clearinghouse(s) 105. Entities... ...that a SC(s) with a signature that can be validated using the public key from the certificate is a valid SC(s).

After the **Electronic Digital** Content Store(s) 103 has received its **digital** certificate that was created by the Clearinghouse(s) 105 and the necessary tools for processing the SC(s) from the **digital** content label, it can begin offering Content 113 that can be purchased by End-User(s). The **Electronic Digital** Content Store(s) 103 includes its certificate and the Transaction SC(s) 640 and signs the SC(s) using its **Digital** Signature 643. The End-User Device(s) 109 verifies that the **Electronic Digital** Content Store(s) 103 is a valid distributor of Content 113 on the Secure **Digital** Content **Electronic** Distribution System 100 by first checking the **digital** certificate revocation list and then using the Public Key 621 of the Clearinghouse(s) 105 to verify the information in the **digital** certificate for the **Electronic Digital** Content Store(s) 103. A **digital** certificate revocation list is maintained by the Clearinghouse(s) 105. The revocation list may be included as one of the parts in a **License** SC(s) 660 that is created by the Clearinghouse(s) 105. End-User Device(s) 109 keep a copy of the revocation list on the End-User Device(s) 109 so they can use it as part of the **Electronic Digital** Content Store(s) 103 **digital** certificate validation. Whenever the End-User Device(s) 109 receives a **License** SC(s) 660 it determines whether a new revocation list is included and if so, the local revocation list on the End-User Device(s) 109 is updated.

B. **Rights** Management Processing

Order SC(s) Analysis

The Clearinghouse(s) 105 receives an Order SC(s) 650 from an End-User(s) after the End-User(s) has received the Transaction SC(s) 640, which include the Offer SC(s) 641, from the **Electronic Digital** Content Store(s) 103. The Order SC(s) 650 consists of parts that contain information relative to the Content 113 and its use, information about the **Electronic Digital** Content Store(s) 103 that is selling the Content 113, and information about the End-User(s) that is purchasing the Content 113. Before the... ...it contains has not been corrupted in any way.

Validation

The Clearinghouse(s) 105 begins the validation of Order SC(s) 650 by verifying the **digital** signatures, then the Clearinghouse(s) 105 verifies the integrity of the Order SC(s) 650 parts. To validate the **digital** signatures, first the Clearinghouse(s) 105 decrypts the Contents 631 of the signature itself using the Public Key 661 of the signing entity included if signed. (The signing entity could be the Content Provider(s) 101, the **Electronic Digital** Content Store(s) 103, the End User Device(s) 109 or any combination of them.) Then, the Clearinghouse(s) 105 calculates the digest of the concatenated part digests of the SC(s) and compares it with the **digital** signature's decrypted Content 113. If

the two values match, the **digital** signature is valid. To verify the integrity of each part, the Clearinghouse(s) 105 computes the digest of the part and compares it to the digest value in the BOM. The Clearinghouse(s) 105 follows the same process to verify the **digital** signatures and part integrity for the Metadata and Offer SC(s) 641 parts included within the Order SC(s) 650.

The process of verification of the Transaction and Offer SC(s) 641 **digital** signatures also indirectly verifies that the **Electronic Digital** Content Store(s) 103 is authorised by the Secure **Digital** Content **Electronic** Distribution System 100. This is based on the fact that the Clearinghouse(s) 105 is the issuer of the certificates. Alternately, the Clearinghouse(s) 105 would be able to successfully verify the **digital** signatures of the Transaction SC(s) 640 and Offer SC(s) 641 using the public key from the **Electronic Digital** Content Store(s) 103, but only if the entity signing the SC(s) has ownership of the associated private key. Only the **Electronic Digital** Content Store(s) 103 has ownership of the private key. Notice that the Clearinghouse(s) 105 does not need to have a local database of the **Electronic Digital** Content Store(s) 103. Since the store uses the Clearinghouse Public Key to sign the Transaction SC(s) 640 Offer SC(s) 641 public keys... ...watermarking instructions are done by the Clearinghouse(s) 105 after authenticity and the integrity check of the Order SC(s) 650, the validation of the **Electronic Digital** Content Store(s) 103, and the validation of the Store Usage Conditions 519 have been completed successfully. The Metadata SC(s) 620 portion of the... ...s) 109 is retrieved from the Order SC(s) 650. The new encrypted Symmetric Keys 623 are included in the Key Description part of the **License** SC(s) 660 that the Clearinghouse(s) 105 returns to the End-User Device(s) 109.

During the time of processing the Symmetric Keys 623... ...the Symmetric Keys 623, the watermarking instructions are modified and re-encrypted. The new watermarking instructions are included as one of the parts within the **License** SC(s) 660 that gets returned to the End-User Device(s) 109.

If all of the processing of the Order SC(s) 650 is successful, then the Clearinghouse(s) 105 returns a **License** SC(s) 660 to the End-User Device(s) 109. The End-User Device(s) 109 uses the **License** SC(s) 660 information to download the Content SC(s) 630 and access the encrypted Content 113 and metadata. The watermarking instructions are also executed... ...to successfully process the Order SC(s) 650, then an HTML page is returned to the End-User Device(s) 109 and displayed in an **Internet** browser window. The HTML page indicates the reason that the Clearinghouse(s) 105 was unable to process the transaction.

In an alternate embodiment, if the user has purchased a copy of the Content 113 prior to the release date set for the sale, the **License**(s) SC 660 is returned without the Symmetric Keys 623. The **License**(s) SC 660 is returned to the Clearinghouse(s) 105 on or after the release date to receive the Symmetric Keys 623. As an example... ...the End-User(s) resides, then the Clearinghouse(s) 105 insures that the transaction being processed is not violating any of those restrictions before transmitting **License** SC(s) 660 to the End-User Device(s) 109. The **Electronic Digital** Content Store(s) 103 is also expected to

participate in managing the distribution of Content 113 to various countries by performing the same checks as the Clearinghouse(s) 105. The Clearinghouse(s) 105 does whatever checking that it can in case the **Electronic Digital** Content Store(s) 103 is ignoring the country specific rules set by the Content Provider(s) 101.

* Audit Logs and Tracking

The Clearinghouse(s) 105... ...during Content 113 purchase transactions and report request transactions. The information can be used for a variety of purposes such as audits of the Secure **Digital** Content **Electronic** Distribution System 100, generation of reports, and data mining.

The Clearinghouse(s) 105 also maintains account balances in Billing Subsystem 182 for the **Electronic Digital** Content Store(s) 103. Pricing structures for the **Electronic Digital** Content Store(s) 103 is provided to the Clearinghouse(s) 105 by the **digital** content labels. This information can include things like current specials, volume discounts, and account deficit limits that need to be imposed on the **Electronic Digital** Content Store(s) 103. The Clearinghouse(s) 105 uses the pricing information to track the balances of the **Electronic Digital** Content Store(s) 103 and insure that they do not exceed their deficit limits set by the Content Provider(s) 101.

The following operations are typically logged by the Clearinghouse(s) 105:

* End-User Device(s) 109 requests for **License** SC(s) 660

* Credit card authorisation number when the Clearinghouse(s) 105 handles the billing

* Dispersement of **License** SC(s) 660 to End-User Device(s) 109

* Requests for reports

* Notification from the End-User(s) that the Content SC(s) 630 and **License** SC(s) 660 were received and validated

The following information is typically logged by the Clearinghouse(s) 105 for a **License** SC(s) 660:

* Date and time of the request

* Date and time of the purchase transaction

* Content ID of the item being purchased

* Identification of the Content Provider(s) 101

* Store Usage Conditions 519

* Watermarking instruction modifications

* Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103

* Identification of the **Electronic Digital** Content Store(s) 103

* Identification of the End-User Device(s) 109

* End-User(s) credit card information (if the Clearinghouse(s) 105 is handling... ...time of the request

* Amount charged to the credit card

* Content ID of the item being purchased

* Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103

* Identification of the **Electronic Digital** Content Store(s) 103

* Identification of the End-User(s)

* End-User(s) credit card information

* Authorisation number received from the clearer of the credit card

The following information is typically logged by the Clearinghouse(s) 105 when a **License** SC(s) 660 is sent to an End-User Device(s) 109:

* Date and time of the request

* Content ID of the item being purchased

* Identification of Content Provider(s) 101

* Usage Conditions 517

* Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103

* Identification of the **Electronic Digital** Content Store(s) 103

* Identification of the End-User(s)

The following information is typically logged when a report request is made:

* Date and time... ...by the Clearinghouse(s) 105 using the information that the Clearinghouse(s) 105 logged during End-User(s) purchase transactions. Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103 can request transaction reports from the Clearinghouse(s) 105 via a Payment Verification Interface 183 so they can reconcile their own... ...with the information logged by the Clearinghouse(s) 105. The Clearinghouse(s) 105 can also provide periodic reports to the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103.

The Clearinghouse(s) 105 defines a secure **electronic** interface which allows Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103 to request and receive reports. The Report Request...that was assigned by the Clearinghouse(s) 105 to the entity initiating the request. The Clearinghouse(s) 105 uses the certificate and the SC's **digital** signature to verify that the request originated from an authorised entity. The request also includes parameters, such as time duration, that define the scope of... ...version of this document.

F. Billing and Payment Verification

Billing of content 113 can be handled either by the Clearinghouse(s) 105 or by the **Electronic Digital** content Store(s) 103. In the case where the Clearinghouse(s) 105 handles the billing of the **electronic** Content 113, the **Electronic Digital** Content Store(s) 103 separates the End-User(s)' order into **electronic** goods and, if applicable, physical goods. The **Electronic Digital** Content Store(s) 103 then, notifies the Clearinghouse(s) 105 of the transaction, including the End-User(s)' billing information, and the total amount that needs to be authorised. The Clearinghouse(s) 105 authorises the End-User(s)' credit card and returns a notification back to the **Electronic Digital** Content Store(s) 103. At the same time the Clearinghouse(s) 105 is authorising the End-User(s)' credit card, the **Electronic Digital** Content Store(s) 103 can charge the End-User(s)' credit card for any physical goods that are being purchased. After each **electronic** item is downloaded by the End-User Device(s) 109, the Clearinghouse(s) 105 is notified so the End-User(s)' credit card can be... ...End- User Device(s) 109 before the Content 113 is enabled for use at the End-User Device(s) 109.

In the case where the **Electronic Digital** Content Store(s) 103 handles the billing of the **electronic** Content 113, the Clearinghouse(s) 105 is not notified about the transaction until the End-User Device(s) 109 sends the Order SC(s) 650 to the Clearinghouse(s) 105. The Clearinghouse(s) 105 is still notified by the End-User Device(s) 109 after each **electronic** item is downloaded. When the Clearinghouse(s) 105 is notified it sends a notification to the **Electronic Digital** Content Store(s) 103 so that the **Electronic Digital** Content Store(s) 103 can charge the End-User(s)' credit card.

G. Retransmissions

The Secure **Digital** Content **Electronic** Distribution System 100 provides the ability to handle retransmissions of Content 113. This is typically performed by a Customer Service Interface 184. **Electronic Digital** Content Store(s) 103 provides a user interface that the End-User(s) can step through in order to initiate a retransmission. The End-User(s) goes to the **Electronic Digital** Content Store(s) 103 site where the Content 113 item was purchased in order to request a retransmission of the Content 113.

Retransmissions of Content... ...a previously purchased Content 113 item because the Content 113 could not be downloaded or the Content 113 that was downloaded is not usable. The **Electronic Digital** Content Store(s) 103 determines whether the End-User(s) is entitled to do a retransmission of the Content 113. If the End-User(s) is entitled to a retransmission, then the **Electronic Digital** Content Store(s) 103 builds a Transaction SC(s) 640 that includes the Offer SC(s) 641 of the Content 113 item(s) being retransmitted... ...s) 109 to delete the scrambled key(s).

In the case where the Clearinghouse(s) 105 handles the financial settlement of Content 113 purchases, the **Electronic Digital** Content Store(s) 103 includes a flag in the Transaction SC(s) 640 that is carried forward to the Clearinghouse(s) 105 in the Order... ...charging the End-User(s) for the purchase of the Content 113.

VIII. CONTENT PROVIDER

A. Overview

The Content Provider(s) 101 in the Secure **Digital** Content **Electronic** Distribution System 100 is the **digital** content label or the entity who owns the **rights** to the Content 113. The role of the Content Provider(s) 101 is to prepare the Content 113 for distribution and make information about the Content 113 available to **Electronic Digital** Content Store(s) 103 or retailers of the downloadable **electronic** versions of the Content 113. To provide the utmost security and **rights** control to the Content Provider(s) 101, a series of tools are provided to enable the Content Provider(s) 101 to prepare and securely package... ...domain and never exposed or accessible by unauthorised parties. This allows Content 113 to be freely distributed throughout a non-secure network, such as the **Internet**, without fear of exposure to hackers or unauthorised parties.

The end goal of the tools for the Content Provider(s) 101 is to prepare and... ...manages the required synchronisation of processes.

* Content Processing Tools 155 - A collection of tools to control Content 113 file preparation including Watermarking, Preprocessing (for an **audio** example any required equalisation, dynamics adjustment, or re-sampling) encoding and compression.

* Metadata Assimilation and Entry Tool 161 - A collection of tools **used** to gather **Content** 113 description information from the Database 160 of the Content Provider(s) and/or third party database or data import files and/or via operator interaction and provides means for specifying content Usage Conditions 517. Also provided is an interface for capturing or extracting content such as **digital audio** content for CDS or DDP files. A Quality Control Tool enables to preview of prepared content and metadata. Any corrections needed to the metadata or... ...to pack into SC(s).

* Content Dispersement Tool (not shown) - Disperses SC(s) to designated distribution centres, such as Content Hosting Site(s) 111 and **Electronic Digital** Content Store(s) 103.

* Content Promotions **Web** Site 156 - stores Metadata SC(s) 620 and optionally additional promotional material for download by authorised **Electronic Digital** Content Store(s) 103.

B. Work Flow Manager 154

The purpose of this tool is to schedule, track, and manage Content 113 processing activities. This... ...or as any of it's constitute processes may be distributed as an application program in a computer readable medium including but not limited to **electronic** distribution such as the **web** or on floppy diskettes, CD ROMS and removable hard disk drives.

Turning now to FIG. 8 is a block diagram of the major processes of... ...information is entered to uniquely identify the product. Optionally, additional fields may be included to request manual entry of the information required to initiate the **audio** processing phase in parallel with the metadata acquisition. If not provided manually, this information can optionally be retrieved from default configuration settings or from the... ...to the Database 160 of the Content Provider(s) 101 is specified, the job is processed by the Automatic Metadata Acquisition Process 803. In a **music** embodiment, to properly schedule the product for **audio** processing, the product's genre and the desired compression levels are specified as well as the **audio** PCM or WAV filename(s). This information may be entered as part of the product selection process or selected via a customised query interface or **Web** browser function. Specification of this information enables the product to be scheduled for content processing.

The product selection user interface provides an option enabling the... ...Manual Metadata Entry Process 804 (see Automatic Metadata Acquisition Process 803 section for details on the Database Mapping Table).

If the required general information for **audio** processing and the specific information required for watermarking is specified, the job is queued for Watermarking Process 808 (the first phase of content processing). If... ...status indicating the information that is missing.

If the status indicates that the filename of the Content 113, for example where the Content 113 is **audio** and the PCM or WAV file is missing, this may indicate that a capture (or **digital** extraction from **digital** media) is required. The **audio** processing functions require that the song files be accessible via a standard file system interface. If the songs are located on external media or a file system that is not directly accessible to the **audio** processing tools, the files are first be copied to an accessible file system. If the songs are in **digital** format but on CD or **Digital** Tape, they are extracted to a file system accessible to the **audio** processing tools. Once the files are accessible, the Work Flow Manager User Interface 700 is used to specify or select the path and filename for...

...Database 160 of the Content Provider(s) 101 to obtain the information necessary to process this Content 113. For example, if the Content 113 is **music**, the information needed to perform this query could be the album name or may be a UPC or a specific album or selection ID as... ...Action/Information Process 801.

6. Supervised Release Process 806

The Supervised Release Process 806 allows a quality check and validation of information specified for the **digital** content product. It does not have any dependencies. Comments previously attached to the job at any stage of the processing for this product can be...

...the usage conditions

* the encryption keys used in the encryption stage of all quality levels for this product

This last dependency requires that the associated **audio** objects completed the **audio** processing phase before the Metadata SC(s) 620 can be created. Upon completion of the Metadata SC(s) Creation Process 807, the job is queued... ...Encryption Process 811.

If third party providers of encoding tools do not provide a method to display the percentage of the Content 113, such as **audio**, that has been processed or a method to indicate the amount of Content 113 that has been encoded as a percentage of the entire selection of Content 113 selected, in FIG. 11 there is shown a flow diagram 1100 of a method to determine the encoding rate of **Digital** Content for the Content Preprocessing and Compression tool of FIG. 8. The method begins with the selection of the desired encoding algorithm and a bit... ...rate factor RNEW)). Calculating a new rate factor RNEW)) knowing the amount of time and the amount of Content 113 encoded is RNEW)) = (length of **Digital** Content encoded)/(amount of time), step 1108. The Content 113 is encoded and the encoding status is displayed using the previously calculate rate factor RNEW... ...of the song file remain available until after Content Quality Control Process 810.

11. Encryption Process 811

The Encryption Process 811 calls the appropriate Secure **Digital** Content **Electronic** Distribution **Rights** Management function to encrypt each of the watermarked/encoded song files. This process has no dependencies other than completion of all other **audio** processing. Upon completion of the Encryption Process 811 process, the job is queued for Content SC(s) Creation Process 812.

12. Content SC(s) Creation... ...onto A1 (New Content Request Process 802).

C. Metadata Assimilation and Entry Tool

Metadata consists of the data describing the Content 113 for example in **music**, title of the recording, artist, author/composer, producer and length of recording. The following description is based upon Content 113 being **music** but it should be understood by those skilled in the art that other content types e.g., video, programs, multimedia, **movies**, and equivalent, are within the true scope and meaning of the present invention.

This Subsystem brings together the data the Content Provider(s) 101 provides to the **Electronic Digital** Content Store(s) 103 to help promote the sale of the product (e.g., for **music**, sample clips by this artist, history of this artist, list of albums on which this recording appears, genres associated with this artist and/or product... ...Provider(s) 101 wants to offer the End-User(s). The data is packaged into a Metadata SC(s) 620 and made available to the **Electronic Digital** Content Store(s) 103. To accomplish this, the following tools are provided:

* Automatic Metadata Acquisition Tool

* Manual Metadata Entry Tool

* Usage Conditions Tool

* Supervised Release... ...to End- User(s) (e.g., composer, producer, sidemen, track length) and the types of promotional data the Content Provider(s) 101 provides to the **Electronic Digital** Content Store(s) 103 (e.g., for a **music** example, sample clips by this artist, a history of this artist, the list of albums on which this recording appears, genres...109, data fields which can be optionally provided to the End-User Device(s) 109 and a sample set of data fields, targeted to the **Electronic Digital** Content Store(s) 103, that promote the artist, album, and/or single.

To extract the template data fields from the Database 160 of the Content... ...user the ability to implement the Usage Conditions Process 805 described above. The process of offering Content 113 for sale or rent (limited use), using **electronic** delivery, involves a series of business decisions. The Content Provider(s) 101 decides at which compression

level(s) the Content 113 is made available. Then for each compressed encoded version of the Content 113, one or more usage conditions are specified. Each usage condition defines the **rights** of the End-User(s), and any restrictions on the End- User(s), with regard to the use of the Content 113.

As part of Content Processing Tools 155, a set of usage conditions (End-User(s) **rights** and restrictions) is attached to the product.

A usage condition defines:

1. the compression encoded version of the Content 113 to which this usage condition... ...condition allows for the purchase or the rental of the Content 113.

For a rental transaction:

the measurement unit which is used to limit the **term** of the rental (e.g., days, plays).

the number of the above units after which the Content 113 will no longer play.

For a purchase... ...the period of time during which the purchase/rental transaction is allowed to occur (i.e., an End-User(s) can purchase/rent under the **terms** of this usage condition only after the beginning availability date and before the last date of availability).

5. the countries from which an End-User... ...the retail channel.

D. Content Processing Tools

The Content Processing Tools 155 is actually a collection of software tools which are used to process the **digital** content file to create watermarked, encoded, and encrypted copies of the content. The tools makes use of industry standard **digital** content processing tools to allow pluggable replacement of watermarking, encoding and encryption technologies as they evolve. If the selected industry tool can be loaded via... ...C/C++ or any equivalent software. The Content Processing Tools 155 can be delivered by any computer readable means including diskettes, CDS or via a **Web** site.

1. Watermarking Tool

The Watermarking Tool provides a user the ability to implement the Watermarking Process 808 as described above. This tool applies copyright information of the Content 113 owner to the song file using **audio** Watermarking technology. The actual information to be written out is determined by the Content Provider(s) 101 and the specific watermarking technology selected. This information... ...requirement on the Metadata Assimilation and Entry Tool 161 to assure that it has acquired this information prior to, for example, allowing the song's **audio** file to be processed. This song will not be available for **audio** processing until the watermarking information has been obtained.

The watermark is applied as the first step in **audio** processing since it is common to all encodings of the song created. As long as the watermark can survive the encoding technology, the watermarking process... ...Preprocessing and Compression Tool

The Preprocessing and Compression Tool provides a user the ability to implement the Preprocessing and Compression Process 809 as described above. **Audio** encoding involves two processes. Encoding is basically the application of a lossy compression algorithm against, for a **music** content example, a PCM **audio** stream. The encoder can usually be tuned to generate various playback bit stream rates based on the level of **audio** quality required. Higher quality results in larger file sizes and since the file sizes can become quite large for high quality Content 113, download times... ...can become lengthy and sometimes prohibitive on standard 28,800 bps modems.

The Content Provider(s) 101 may, therefore, choose to offer a variety of **digital** content qualities for download to appease both the impatient and low bandwidth customers who don t want to wait hours for a download and the... ...to the compression algorithm. To allow for more efficient compression with less loss of fidelity or to prevent drastic dropout of some frequency ranges, the **digital** content may sometimes require adjustments to equalisation levels of certain frequencies or adjustments to the dynamics of the recording. The content preprocessing requirements are directly related to the compression algorithm and the level of compression required. In some cases, the style of Content 113 (e.g. **musical** genre) can be successfully used as a base for determining preprocessing requirements since songs from the same genre typically have similar dynamics. With some compression tools, these preprocessing functions are part of the encoding process. With others, the desired preprocessing is performed prior to the compression.

Besides the downloadable **audio** file for sale, each song also has a Low Bit Rate (LBR) encoded clip to allow the song to be sampled via a LBR streaming... ...compression. The front end Encoding Tool may have a synchronisation requirement with the Metadata Assimilation and Entry Tool 161, for example if the content is **music**, and if it is determined that the song's genre is acquired from the Database 160 of the Content Provider(s) prior to performing any **audio** preprocessing. This depends on the encoding tools selected and how indeterminate the genre for the song is. If the Content Provider(s) 101 varies the... ...present invention. The process starts with reading an identifier from the media the Content Provider(s) 101 is examining. One example of content in an **audio** CD embodiment. In an **audio** CD embodiment, the following codes may be available

Universal Price Code (UPC), International Standard Recording Code (ISRC), International Standard **Music** Number (ISMN). This identifier is read in the appropriate player for the content, for example an **audio** CD Player for **audio** CD, DVD player for DVD **movie**, DAT recorder for DAT recording and equivalent, step 1201. Next this Identifier is used to index a Database 160 for the Content Provider(s) 101... ...113 and the metadata related to it. In step 1204, the additional information retrieved is used to start the Work Flow Manager 154 for creating **electronic** Content 113. It should be understood, that several selections of media, such as several **audio** CDS, can be queued up so as to enable the Automatic Metadata Acquisition Tool to create a series of Content 113 for **electronic** distribution. For example, all the Content 113 could be created from a series of CDS or even selected tracks from one or more CDS examined... ...Preprocessing and Compression parameters of the Preprocessing and Compression Tool of FIG. 8 according to the present invention. In this embodiment, the Content 113 is **music**. In step 1301, **music** (Content 113) is selected to be encoded in Content Processing Tools 155. The genre of the **music** selected is determined, step 1302. This can be entered manually or by using other meta data available, such as the additional data retrieved from the process described in FIG. 12. The **audio** compression level and **audio** compression algorithms selected are than examined, step 1303. Next, a lookup is made by genre, compression settings and compression algorithms of what compression parameters should... ...630. This process creates a single Metadata SC(s) 620 and multiple Content SC(s) 630 for each song. For example, if the content is **music**, each of the **audio** files created during **audio** processing for the various quality levels of the full song is packed into separate Content SC(s) 630. The **audio** file created for the sample clip is passed as a metadata file to be included in the Metadata SC(s) 620.

F. Final Quality Assurance... ...101 can choose to perform quality assurance as each major step is completed to prevent excessive rework later or may choose to wait until all **audio** preparation processes are complete and perform quality assurance on everything at once. If the latter is chosen, quality assurance is performed at this point upon completion of the creation of the SC(s). This tool allows each SC(s) for the song to be opened, examined, and the **audio** played.

Any problem discovered, even minor text changes requires that the SC(s) be rebuilt due to internal security features of SC(s). To avoid... ...101 to prepare content in advance of their scheduled release date and hold them until they wish to release them e.g., a new song, **movie** or game. The SC(s) can also control access to Content 113 based on a defined release date so there is no requirement for the... ...are transferred via FTP to the designated Content Hosting Site(s) 111. The Metadata SC(s) 620 is transferred via FTP to the Content Promotions **Web** Site 156. Here the SC(s) are staged to a new Content 113 directory until they can be processed and integrated into the Content Promotions **Web** Site 156.

FIG. 17 is a flow diagram of an alternate embodiment to automatically retrieve additional information for the Automatic Metadata Acquisition Tool of FIG... ...Manual Metadata

Entry 803. Since, many of the usage conditions can be automatically filled-in during the Automatic Metadata Acquisition 803 step.

H. Content Promotions **Web** Site

To most effectively disperse information on what the Content Provider(s) 101 is making available for sale via **digital** download, and to get the necessary files to the **Electronic Digital** Content Store(s) 103 to enable it to make this Content 113 available for download to its customers, each Content Provider(s) 101 should have a secure **web** site housing this information. This is similar to the method used today by some Content Provider(s) 101 to make promotional content available to their... ...others with a need for this information. In the case where this type of service already exists, an additional section can be added to the **web** site where **Electronic Digital** Content Store(s) 103 can go to see a list of the content available for sale via download.

The Content Provider(s) 101 has complete control over the design and layout of this site or can choose to use a turnkey **web** server solution provided as part of the toolkit for Secure **Digital** Content **Electronic** Distribution System 100. To implement their own design for this service, the Content Provider(s) 101 need only provide links to the Metadata SC(s) 620 for **Electronic Digital** Content Store(s) 103 who access their site. This is accomplished using the toolkit for the Secure **Digital** Content **Electronic** Distribution System 100. The selection process and what information is shown is the discretion of the Content Provider(s) 101.

Metadata SC(s) 620 received into a new content directory via FTP from the Content Dispersement Tool is processed by the Content Promotions **Web** Site 156. These containers can be opened with the SC(s) Preview Tool to display or extract information from the container. This information can then be used to update HTML **Web** pages and/or add information to a searchable database maintained by this service. The SC(s) Preview Tool is actually a subset of the **Content** Acquisition Tool **used** by the **Electronic Digital** Content Store(s) 103 to open and process Metadata SC(s) 620. See the Content Acquisition Tool section for more details. The Metadata SC(s) 620 file should then be moved to a permanent directory maintained by the Content Promotions **Web** Site 156.

Once the Metadata SC(s) 620 has been integrated into the Content Promotions **Web** Site 156, its availability is publicised. The Content Provider(s) 101 can send a notification to all subscribing **Electronic Digital** Content Store(s) 103 as each new Metadata SC(s) 620 is added to the site or can perform a single notification daily (or any defined periodicity) of all Metadata SC(s) 620 added that day (or period). This notification is performed via a standard HTTP exchange with the **Electronic Digital** Content Store(s) 103 **Web** Server by sending a defined CGI string containing parameters referencing the Metadata SC(s) 620 added. This message is handled by the Notification Interface Module of the **Electronic Digital** Content Store(s) 103 which is described later.

I. Content Hosting

The Entertainment Industry produces thousands of content titles, such as CDS, **movies** and games every year, adding to the tens of thousands of content titles that are currently available. The Secure **Digital** Content **Electronic** Distribution System 100 is designed to support all of the content titles available in stores today.

The numbers of content titles that the Secure **Digital** Content **Electronic** Distribution System 100 may eventually download to customers on a daily basis is in the thousands or tens of thousands. For a large number of... ...The system also supports customers all over the world. This requires overseas sites to speed delivery to the global customers.

Content hosting on the Secure **Digital** Content **Electronic** Distribution System 100 is designed to allow the Content Provider(s) 101 to either host their own Content 113 or share a common facility or a set of facilities.

Content hosting on the Secure **Digital** Content **Electronic** Distribution System 100 consists of multiple Content Hosting Site(s) 111 that collectively contain all of the Content 113 offered by the Secure **Digital** Content **Electronic** Distribution System 100 and several Secondary Content Sites (not shown) that contain the current hot hits offered by the Content Provider(s) 101. The number... ...single Content Hosting Site 111 with or without additional Secondary Content Sites. This allows them to build their own scalable distributed system. In another embodiment, **Electronic Digital** Content Store(s) 103 can also act as Content Hosting Site(s) 111 for certain Content 113. This embodiment requires a special financial agreement between the **Electronic Digital** Content Store(s) 103 and the Content Provider(s) 101.

1. Content Hosting Sites

Content 113 is added to the Content Hosting Site(s) 111... ...field that indicates the URL locating the Content SC(s) 630 for this Content 113. This URL corresponds to a Content Hosting Site(s) 111. **Electronic Digital** Content Store(s) 103 can override this URL if allowed by the Content Provider(s) 101 in the Offer SC(s) 641. The End-User... ...to download the Content SC(s) 630.

The End-User Device(s) 109 initiates the request for a Content SC(s) 630 by sending the **License** SC(s) 660 to the Content Hosting Site(s) 111. This is the same **License** SC(s) 660 returned by the Clearinghouse(s) 105. The **Digital** Signature of the **License** SC(s) 660 can be verified to determine if it is a valid **License** SC(s) 660. If it is a valid **License** SC(s) 660 either the download is initiated, or the download request may be redirected to another Content Hosting Site(s) 111.

2. Content Hosting Site(s) 111 provided by the Secure **Digital** Content **Electronic** Distribution System 100

For the Secure **Digital** Content **Electronic** Distribution System 100 the decision of which site should be used to download the Content 113 is made by the primary content site that received... ...information to make this decision:

* Are there secondary content sites that host the Content 113 requested? (The majority of Content 113 offered by the Secure **Digital** Content **Electronic** Distribution System 100 is only located at primary sites);

* Where is the End-User Device(s) 109 geographically located? (This information can be obtained from... ...the End-User Device(s) 109, analysis and verifications are performed on the End-User's request. A database is kept of all of the **License** SC IDs that have been **used** to download **Content** 113. This database can be checked to ensure that the End-User Device(s) 109 only makes one request for each piece of Content 113... ...the amount of activity on the sites and whether a site is down for maintenance.

The only interface to the Content Hosting Router is the **License** SC(s) 660 that is sent by the End-User Device(s) 109 when Content 113 is required to be downloaded. The **License** SC(s) 660 includes information that indicates the user is allowed to download the Content 113.

Secondary Content Sites

The Secondary Content Sites (not shown) host the popular Content 113 of the Secure **Digital** Content Distribution System 100. These sites are geographically dispersed across the world and are located near Network Access Points (NAPS) to improve download times. These sites are added to the system as demand on the primary Content Hosting Site(s) 111 nears maximum capacity

IX. **ELECTRONIC DIGITAL** CONTENT STORE(S)

A. Overview - Support for Multiple **Electronic Digital** Content Store(s) 103

Electronic Digital Content Store(s) 103 are essentially the retailers. They are the entities who market the Content 113 to be distributed to the customer. For distribution of Content 113, this would include **Digital** Content Retailing **Web** Sites, **Digital** Content Retail

Stores, or any business who wishes to get involved in marketing **electronic** Content 113 to consumers. These businesses can market the sale of **electronic** Content 113 only or can choose to just add the sale of **electronic** goods to whatever other merchandise they currently offer for sale. Introduction of downloadable **electronic** goods into the service offering of the **Electronic Digital** Content Store(s) 103 is accomplished via a set of tools developed for the **Electronic Digital** Content Store(s) 103 as part of the Secure **Digital** Content **Electronic** Distribution System 100. These tools are used by the **Electronic Digital** Content Store(s) 103 to:

* acquire the Metadata SC(s) 620 packaged by the Content Provider(s) 101

* extract Content 113 from these SC(s... ...the status of each download

* handle status notifications and transaction authentication requests

* perform account reconciliation

The tools are designed to allow flexibility in how the **Electronic Digital** Content Store(s) 103 wishes to integrate sale of downloadable **electronic** Content 113 into its service. The tools can be used in such a way as to request that all financial settlements for downloadable Content 113 purchased be handled by the Clearinghouse(s) 105 although this is not required. These tools also enable **Electronic Digital** Content Store(s) 103 to completely service their customers and handle the financial transactions themselves, including providing promotions and special offers. The tools enable the **Electronic Digital** Content Store(s) 103 to quickly integrate the sale of downloadable Content 113 into its existing services. In addition, the **Electronic Digital** Content Store(s) 103 is not required to host the downloadable Content 113 and does not have to manage its dispersement. This function is performed by the Content Hosting Site(s) 111 selected by the Content Provider(s) 101.

The tools for the **Electronic Digital** Content Stores(s) 103 are implemented in Java in the preferred embodiment but other programming languages such as C/C++, Assembler and equivalent can be used. It should be understood that the tools described below for the **Electronic Digital** Content Stores(s) 103 can run on a variety of hardware and software platforms. The **Electronic Digital** Content Stores(s) 103 as a complete system or as any of it's constitute components may be distributed as an application program in a computer readable medium including but not limited to **electronic** distribution such as the **web** or on floppy diskettes, CD ROMS and removable hard disk drives.

In another embodiment, the components of the **Electronic Digital** Content Stores(s) 103 is part of a programmer's software toolkit. This toolkit enables predefined interfaces to the components of the generic **Electronic Digital** Content Stores(s) 103 components and tools discussed below. These predefined interfaces are in the form of APIs or Application Programming Interfaces. A developer using... ...of the functionality of the components from a high level application program. By providing APIs to these components, a

programmer can quickly develop a customised **Electronic Digital** Content Stores(s) 103 without the need to re-created these functions and resources of any of these components.

Electronic Digital Content Store(s) 103 are not limited to **Web** based service offerings. The tools provided are used by all **Electronic Digital** Content Store(s) 103 wishing to sell downloadable **electronic** Content 113 regardless of the transmission infrastructure or delivery mode used to deliver this Content 113 to End-User(s). Broadcast services offered over satellite and cable infrastructures also use these same tools to acquire, package, and track **electronic** Content 113 sales. The presentation of **electronic** merchandise for sale and the method in which these offers are delivered to the End-User(s) is the main variant between the broadcast based service offering and the point-to-point interactive **web** service type offering.

B. Point-to-Point **Electronic Digital** Content Distribution Service

Point-to-Point primarily means a one-to-one interactive service between the **Electronic Digital** Content Store(s) 103 and the End-User Device(s) 109. This typically represents an **Internet web** based service provided via telephone or cable modem connection. Networks other than the **Internet** are supported in this model as well, as long as they conform to the **Web** Server/Client Browser model. FIG. 9 is a block diagram illustrating the major tools, components and processes of an **Electronic Digital** Content Store(s) 103.

1. Integration Requirements

The Secure **Digital** Content **Electronic** Distribution System 100 not only creates new **online** businesses but provides a method for existing businesses to integrate the sale of downloadable **electronic** Content 113 to their current inventory. The suite of tools provided to the **Electronic Digital** Content Store(s) 103 simplify this integration effort. The Content Acquisition Tool 171 and SC(s) Packer Tool 153 provides a method for the **Electronic Digital** Content Store(s) 103 to acquire information from the participating Content Provider(s) 101 on what they have available for sale and to create the... ...is batch driven and can be largely automated and is executed only to integrate new Content 113 into the site.

The tools for the Secure **Digital** Content **Electronic** Distribution have been designed to allow integration of sale of **electronic** downloadable Content 113 into typical implementations of **web** based **Electronic Digital** Content Store(s) 103 (i.e. Columbia House **online**, **Music** Boulevard, @Tower) and equivalent with minimal change to their current Content 113 retailing paradigm. Several methods of integration are possible and in the preferred embodiment, the **Electronic Digital** Content Store(s) 103 provides support for all product searches, previews, selections (shopping cart), and purchases. Each **Electronic Digital** Content Store(s) 103 establishes customer loyalty with its

customers and continues to offer its own incentives and market its products as it does today. In the Secure **Digital** Content **Electronic** Distribution System 100, it would simply need to indicate which products in its inventory are also available for **electronic** download and allow its customers to select the **electronic** download option when making a purchase selection. In another embodiment, the customer's shopping cart could contain a mixture of **electronic** (Content 113) and physical media selections. After the customer checks out, and the **Electronic Digital** Content Store(s) 103 has completed the financial settlement and logged or notified its shipping and handling functions to process the physical merchandise purchased, the commerce handling function of the **Electronic Digital** Content Store(s) 103 then calls the Transaction Processor Module 175 to handle all **electronic** downloads. It simply passes the required information and all processing from that point on is handled by the toolset for the Secure **Digital** Content **Electronic** Distribution System 100. In another embodiment, other methods of transaction handling are also possible using tools for the Secure **Digital** Content **Electronic** Distribution System 100 to handle the financial settlement should the **Electronic Digital** Content Store(s) 103 wish to sell downloadable merchandise only or to segregate the financial settlement of physical and downloadable merchandise.

To handle the downloading of merchandise, the **Electronic Digital** Content Store(s) 103 is given a Product ID (not shown) for each downloadable product that it acquires from the Content Promotions **Web** Site 156 for the Content Provider(s) 101. This Product ID is associated to a customer's purchase selection to the downloadable product. The Product ID is what the **Electronic Digital** Content Store(s) 103 passes to the Transaction Processor Module 175 to identify the product that the user has purchased. The SC(s) (Offer SC(s) 641) that were created to describe the products, are isolated from the **Electronic Digital** Content Store(s) 103 and kept in an Offer Database 181 in an effort to simplify management of these objects and make their existence transparent to the **Electronic Digital** Content Store(s) 103.

The Transaction Processor Module 175 and other additional functions are provided as **web** server side executables (i.e. CGI and NSAPI, ISAPI callable functions) or simply APIs into a DLL or C object library. These functions handle run time processing for End-User(s) interactions and optional interactions with the Clearinghouse(s) 105. These functions interact with the **web** server's commerce services to create and download to the End-User Device(s) 109 the files necessary to initiate the Content 113 download process... ...also handle optional interactions to provide authorisations and accept notifications of completion of activities.

An Accounting Reconciliation Tool 179 is also provided to assist the **Electronic Digital** Content Store(s) 103 in contacting the Clearinghouse(s) 105 to reconcile accounts based on its own and the transaction logs of the Clearinghouse(s) 105.

2. Content Acquisition Tool 171

The Content Acquisition Tool 171 is responsible for interfacing with the Content Promotions **Web** Site 156 to preview and download Metadata SC(s) 620. Since the Content Promotions site is a standard **web** site, a **web** browser is used by the **Electronic Digital** Content Store(s) 103 to navigate this site. The navigation features varies based on the site design of the Content Provider(s) 101. Some sites... ...from. All sites include the selection of Metadata SC(s) 620 containing all the promotional and descriptive information of a song or album.

Alternatively, the **Electronic** Store(s) 103 may subscribe to content updates and receive updates automatically via FTP.

Viewing Metadata

The Content Acquisition Tool 171 is a **web** browser helper application which launches whenever a Metadata SC(s) 620 link is selected at the Content Promotions **Web** Site 156. Selection of the SC(s) causes it to be downloaded to the **Electronic Digital** Content Store(s) 103, and launch the helper application. The Content Acquisition Tool 171 opens the Metadata SC(s) 620 and display the non-encrypted information contained therein. Displayed information includes Extracted Metadata 173, for a **music** example, the graphic image(s) associated with the song and the information describing the song, a preview clip of the song can also be listened to if included in the Metadata SC(s) 620. In an example where the Content 113 is **music**, promotional information about the song or album, the album title, and the artist is also shown if provided by the Content Provider(s) 101. This... ...as the song and the lyrics and whatever other metadata the Content Provider(s) 101 wishes to protect, is not accessible to the Retail Content **Web** Site 180.

In another embodiment, the Content Provider(s) 101 provides optional promotional content for a fee. In this embodiment such promotional content is encrypted in the Metadata SC(s) 620. Financial settlement to open this data can be handled via the Clearinghouse(s) 105 with the account for the **Electronic Digital** Content Store(s) 103 being charged the designated fee.

Extracting Metadata

Besides the preview capabilities, this tool provides two additional features: metadata extraction and preparation of an Offer SC(s) 641. Selection of the metadata extraction option prompts the **Electronic Digital** Content Store(s) 103 to enter the path and filenames to where the metadata is to be stored. Binary metadata such as graphics and the **audio** preview clip is stored as separate files. Text metadata is stored in an ASCII delimited text file which the Retail Content **Web** Site 180 can then import into its database. A table describing the layout of the ASCII delimited file is also be created in a separate... ...One important piece of information provided in the extracted data is the

Product ID. This Product ID is what the commerce handling function for the **Electronic Digital** Content Store(s) 103 needs to identify to the Transaction Processor Module 175 (for more information refer to Transaction Processing section), the Content 113 that...
...to properly retrieve the appropriate Offer SC(s) 641 from the Offer Database 181 for subsequent download to the End-User Device(s) 109. The **Electronic Digital** Content Store(s) 103 has full control over how it presents the offer of downloadable Content 113 on its site. It only needs to retain a cross reference of the Content 113 being offered to this Product ID to properly interface with the tools for the Secure **Digital** Content **Electronic** Distribution System 100. Providing this information here, allows the **Electronic Digital** Content Store(s) 103 to integrate this product or Content 113 into its inventory and sales pages (database) in parallel with the Offer SC(s... ...process since both processes uses the same Product ID to reference the product. This is described further below.

Offer SC(s) Creation Packer 153

The **Electronic Digital** Content Store(s) 103 is required to create an Offer SC(s) 641 describing the downloadable Content 113 that is for sale. Most of the... ...Template in the Metadata SC(s) 620

* adding additional required parts as defined by defaults specified by the configuration options in this tool for the **Electronic Digital** Content Store(s) 103

* prompting for additional required inputs or selections as defined by the Offer SC(s) Template in the Metadata SC(s) 620... ...later) on the End-User Device(s) 109 is kept in the Metadata SC(s) 620. Other promotional metadata that was only used by the **Electronic Digital** Content Store(s) 103 as input to his **web** service database is removed from the Metadata SC(s) 620. **Rights** management information provided by the Content Provider(s) 101, such as watermarking instructions, encrypted Symmetric Keys 623, and Usage Conditions 517 defining the permitted uses of the object, are also retained.

This stripped down Metadata SC(s) 620 is then included in the Offer SC(s) 641. The **Electronic Digital** Content Store(s) 103 also attaches its own Usage Conditions called Store Usage Conditions 519 or purchase options to the Offer SC(s) 641. This can be accomplished interactively or automatically through a set of defaults. If configured to be processed interactively, the **Electronic Digital** Content Store(s) 103 is prompted with the set of permitted object Usage Conditions 517 as defined by the Content provider(s) 101. He then... ...option(s) he wishes to offer to his customers. These now become the new Usage Conditions or Store Usage Conditions 519. To process automatically, the **Electronic Digital** Content Store(s) 103 configures a set of default purchase options to be offered for all Content 113. These default options are automatically checked against... ...Database 181 and is indexed with the Product ID pre-assigned in the Metadata SC(s) 620. This Product ID is used later by the **Electronic Digital** Content Store(s) 103 to identify the downloadable Content 113 being purchased by a customer when interfacing

with the Offer Database 181 to retrieve the... ...s) 641 for packaging and transmittal to the End-User(s). See the Transaction Processor Module 175 section for more details.

In another embodiment, the **Electronic Digital** Content Store(s) 103 hosts the Content SC(s) 641 at his site. This embodiment requires changes to the Offer SC(s) 641 such as the replacement of the URL of the Content Hosting Site(s) 111 with the URL of the **Electronic Digital** Content Store(s) 103.

3. Transaction Processing Module 175

Electronic Digital Content Store(s) 103 directs billing to Clearinghouse(s) 105. Alternatively, the **Electronic Digital** Content Store(s) 103 may request financial clearance direct from the Clearinghouse(s) 105. There are two basic modes for processing End-User(s) purchase requests for downloadable Content 113. If the **Electronic Digital** Content Store(s) 103 does not wish to handle the financial settlement of the purchase and has no special promotions or incentives governing the sale... ...pricing information included in the metadata. Also included in the Offer SC(s) 641 is a special HTML offer page presenting the purchase options with **terms** and conditions of the sale. This page is built from a template created when the Offer SC(s) 641 was built. When the End- User... ...this form may contain the fields needed to use the End-User(s)' credit information or industry standard local transaction handler.

An embodiment where the **Electronic Digital** Content Store(s) 103 handles billing is now described. The more typical mode of handling purchase requests is to allow the **Electronic Digital** Content Store(s) 103 to process the financial settlement and then submit the download authorisation to the End-User(s). This method allows the **Electronic Digital** Content Store(s) 103 to integrate sale of downloadable Content 113 with other merchandise offered for sale at his site, allows batch processing of purchase requests with only one consolidated charge to the customer (via a shopping cart metaphor) instead of individual charges for each download request, and allows the **Electronic Digital** Content Store(s) 103 to directly track his customers buying patterns and offer special promotions and club options. In this environment, the offer of downloadable... ...which get added to a shopping cart when selected by the End-User(s) and get processed and financially settled as is done in the **Electronic Digital** Content Store(s)' 103 current shopping model. Once the financial settlement is completed, the commerce handling process of the **Electronic Digital** Content Store(s) 100 then calls the Transaction Processor Module 175 to complete the transaction.

Transaction Processor Module 175

The role of the Transaction Processor... ...113 purchased. This information is packaged into a Transaction SC(s) 640 which is sent back to the End-User Device(s) 109 by the

Web Server as the response to the purchase submission. The Transaction Processor Module 175 requires three pieces of information from the commerce handling process of the **Electronic Digital** Content Store(s) 103: the Product IDs for the Content 113 purchased, Transaction Data 642, and an HTML page or CGI URL acknowledging the purchase settlement.

The Product ID is the value provided to the **Electronic Digital** Content Store(s) 103 in the Metadata SC(s) 620 associated to the Content 113 just sold. This Product ID is used to retrieve the... ...SC(s) 641 from the Offer Database 181.

The Transaction Data 642 is a structure of information provided by the transaction processing function of the **Electronic Digital** Content Store(s) 103 which is later used to correlate the Clearinghouse(s) 105 processing with the financial settlement transaction performed by the **Electronic Digital** Content Store(s) 103 and to provide user identity information to be included in the watermark of the Content 113 downloaded to the End-User... ...109. When the Clearinghouse(s) 105 receives a valid Order SC(s) 650, it logs a transaction indicating the Content 113 that was sold, which **Electronic Digital** Content Store(s) 103 sold it and the associated Transaction Data 642 including the End-User's Name and a Transaction ID 535. The Transaction ID 535 provides a reference to the financial settlement transaction. This information is later returned by the Clearinghouse(s) 105 to the **Electronic Digital** Content Store(s) 103 for use in reconciling its accounts with the billing statements received from the Content Provider(s) 101 (or his agent). The Clearinghouse Transaction Log 178 can be **used** by the **Content** Provider(s) 101 to determine what Content 113 of his has been sold and enables him to create a bill to each **Electronic Digital** Content Store(s) 103 for royalties owed him. Other **electronic** means besides billing can alternatively be used to settle accounts between the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103.

The information provided in the Transaction SC(s) 640 and the security and integrity of the Transaction SC(s) 640 provide... ...the purchase transaction is valid and thus no further validation is required prior to the logging of this sale by the Clearinghouse(s) 105. The **Electronic Digital** Content Store(s) 103, however, has the option to request authentication before its accounts are charged (transaction logged at the Clearinghouse(s) 105 indicating to the Content Provider(s) 101 that this **Electronic Digital** Content Store(s) 103 has collected money for the sale of this Content 113). This request for authentication/notification is indicated by a flag in the Transaction Data 642. In this scenario, the Clearinghouse(s) 105 contacts the **Electronic Digital** Content Store(s) 103 and receive authorisation from the **Electronic Digital** Content Store(s) 103 before the charge to his account and the release of the encryption Key 623. The Transaction ID 535 is passed to the **Electronic Digital** Content Store(s) 103 from the Clearinghouse(s) 105 as part of this authentication request to enable the **Electronic Digital** Content Store(s) 103 to associate this request to a prior transaction performed with the End-User(s). This Transaction ID 535 can be any unique value the **Electronic Digital** Content Store(s) 103 wishes to use and is solely for its benefit.

The Transaction Data 642 also contains a customer name. This name can... ...of the purchase form filled out by the user when making his purchase, or from information logged previously during some user registration process with the **Electronic Digital** Content Store(s) 103, or the official name obtained from credit card information associated with the card used in this transaction. This name is later included in the **License** Watermark 527.

The Transaction Data 642 also contains the Store Usage Conditions 519 purchased by the End-User(s). This information is included in the **License** Watermark 527 and used by the End- User Device(s) 109 in Copy and Play Control.

The final parameter required by the Transaction Processor Module 175 is the HTML page or CGI URL acknowledging the purchase settlement. The purpose of this is to allow the **Electronic Digital** Content Store(s) 103 to respond to the End-User(s) with an acknowledgement of the financial settlement and whatever other information he wishes to... ...the Transaction SC(s) 640 is received and processed.

The Transaction SC(s) 640 is the HTTP response to the End-User(s) from the **Electronic Digital** Content Store(s) 103 after processing the purchase submission. Sending a SC(s) as the direct HTTP response forces the automatic loading on the End... ...use by the Notification Interface Module 176 and the Account Reconciliation Tool 179.

4. Notification Interface Module 176

The Notification Interface Module 176 is a **Web** Server side executable routine (CGI or function callable by NSAPI, ISAPI or equivalent). It handles optional requests and notifications from the Clearinghouse(s) 105, the End-User Device(s) 109, the Content Hosting Site(s) 111, and the Content Provider(s) 101. The events that the **Electronic Digital** Content Store(s) 103 can optionally request notification for are:

* Notification from the Clearinghouse(s) 105 that the End-User Device(s) 109 requested an... ...Clearinghouse(s) 105 is releasing the encryption Key 623 for the specified Content 113. This notification can optionally be configured to require authentication from the **Electronic Digital** Content Store(s) 103 prior to the encryption Key 623 being sent to the End-User Device(s) 109.

* Notification from the Content Hosting Site... ...been sent to the End-User Device(s) 109.

* Notification from the End-User Device(s) 109 that the Content SC(s) 630 and the **License** SC(s) 660 have been received and successfully used to process the Content 113 or was found to be corrupt.

* Notification from the Content Provider(s) 101 that new Content 113 has been placed in the Content Promotions **Web** Site 156.

None of these notifications are a required step in the Secure **Digital** Content **Electronic** Distribution System flows 100 but are provided as options to allow the **Electronic Digital** Content Store(s) 103 the opportunity to close its records on the satisfaction of completion of the sale. It also provides information that may be needed to handle customer service requests by letting the **Electronic Digital** Content Store(s) 103 know what functions have transpired since financial settlement of the transaction or what errors occurred during an attempt to complete the... ...from the Clearinghouse(s) 105 through the Customer Service Interface 184 as needed.

Frequency of notification of new Content 113 available at the Content Promotions **Web** Site 156 is determined by the Content Provider(s) 101. Notification may be provided as each new Metadata SC(s) 620 is added or lust... ...all new Metadata SC(s) 620 added that day.

All of these notifications result in entries being made to the Transaction Log 178. If the **Electronic Digital** Content Store(s) 103 wishes to perform his own processing on these notifications, he can intercept the CGI call, perform his unique function and then... ...to compare the Transaction Log 178 with the log of the Clearinghouse(s) 105. This is an optional process which is available to help the **Electronic Digital** Content Store(s) 103 feel comfortable with the accounting for the Secure **Digital** Content **Electronic** Distribution System 100.

In another embodiment, this tool can be updated to provide **electronic** funds transfers for automated periodic payments to the Content Provider(s) 101 and the Clearinghouse(s) 105. It can also be designed to automatically process payments upon reception of an **electronic** bill from the Clearinghouse(s) 105 after reconciling the bill against the Transaction Log 178.

C. Broadcast **Electronic Digital** Content Distribution Service

Broadcast primarily refers to a one to many transmission method where there is no personal interaction between the End-User Device(s) 109 and the **Electronic Digital** Content Store(s) 103 to customise on-demand viewing and listening. This is typically provided over a **digital** satellite or cable infrastructure where the Content 113 is preprogrammed so that all End-User Device(s) 109 receive the same stream.

A hybrid model can also be defined such that an **Electronic Digital** Content Store(s) 103 provides a **digital** content service organised in such a way that it can offer both a **web** distribution interface via an **Internet** connection as well as a higher bandwidth satellite or cable distribution interface via a broadcast service, with a great deal of commonality to the site design. If the IRD backchannel serial interface were connected to the **web**, and

the IRD supported **web** navigation, the End-User(s) could navigate the **digital** content service in the usual way via the backchannel **Internet** interface, previewing and selecting Content 113 to purchase. The user can select high quality downloadable Content 113, purchase these selections, and receive the required **License** SC(s) 660 all via an **Internet** connection and then request delivery of the Content 113 (Content SC(s) 630) over the higher bandwidth broadcast interface. The **Web** service can indicate which Content 113 would be available for download in this manner based on the broadcast schedule or could build the broadcast streams based totally on purchased Content 113. This method would allow a **Web** based **digital** content service to contract with a broadcast facility to deliver high quality Content 113 to users equipped with the proper equipment making a limited number... ...specific Content 113 (e.g. songs or CDS) available daily in this manner and the entire catalog available for download in lower quality via the **web** interface.

Other broadcast models can be designed where there is no **web** interface to the End-User Device(s) 109. In this model, promotional content is packaged in specially formatted **digital** streams for broadcast delivery to the End-User Device(s) 109 (i.e. IRD) where special processing is performed to decode the streams and present... ...End-User Device(s) 109 to the Clearinghouse(s) 105 and would utilise SC(s) to perform all data exchange. The toolset provided to the **Electronic Digital** Content Store(s) 103 has been architected and developed in such a way that most of the tools apply to both a point-to-point **Internet** service offering as well as a broadcast satellite or cable offering. The tools used by a **Digital** Content **Web** Site **Electronic Digital** Content Store(s) 103 to acquire and manage Content 113 as well as prepare SC(s) is also used by a satellite based **Electronic Digital** Content Store(s) 103 to manage and prepare Content 113 for distribution on a broadcast infrastructure. The SC(s) distributed over a **Web** service are the same as those distributed over a broadcast service.

X. applications in the End-User Device(s) 109 for the Secure **Digital** Content **Electronic** Distribution System 100 perform two main functions: first the SC(s) processing and copy control; and second playback of encrypted Content 113. Whether the End-User Device(s) 109 is a Personal Computer or a specialised **electronic** consumer device, it has to be capable of performing these base functions. The End-User Device(s) 109 also provides a variety of additional features and functions like creating play lists, managing the **digital** content library, displaying information and images during content playback, and recording to external media devices. These functions vary based on the services these applications are... ...FIG. 10, shown is the major components and processes and End-User Device(s) 109 Functional Flow. The applications designed to support a PC based **web** interface Content 113 service consists of two executable software applications: the SC(s) Processor 192 and the Player Application 195. The SC(s) Processor 192 is an executable application which is configured as a Helper Application into the End-User(s) **Web** Browser 191 to handle SC(s) File/MIME Types. This application is launched by the Browser whenever SC(s) are received from the **Electronic Digital** Content Store(s) 103, the Clearinghouse(s) 105, and the Content Hosting Site(s) 111. It is responsible for

performing all required processing of the SC(s) and eventually adding Content 113 to the **Digital** Content Library 196 of the End-User(s).

The Player Application 195 is a stand alone executable application which the End-User(s) loads to perform Content 113 in his **Digital** Content Library 196, manage his **Digital** Content Library 196 and create copies of the Content 113 if permitted. Both the Player Application 195 and SC(s) Processor 192 applications can be... ...and browsing of Content 113 information, previewing of, for example, song clips, and selecting songs for purchase is all handled via the End-User(s) **Web** Browser 191. **Electronic Digital** Content Store(s) 103 provides the shopping experience in the same way that is offered today by many Content 113 retailing **web** sites. The difference to the End-User(s) over today's **web** based Content 113 shopping is that they may now select downloadable Content 113 objects to be added to their shopping cart. If the **Electronic Digital** Content Store(s) 103 has other merchandise available for sale in addition to the downloadable objects, the End-User(s) may have a combination of physical and **electronic** downloadable merchandise in his shopping cart. The Secure **Digital** Content **Electronic** Distribution End-User Device(s) 109 are not involved until after the End-User(s) checks out and submits his final purchase authorisation to the **Electronic Digital** Content Store(s) 103. Prior to this point, all interaction is between the **Web** Server for the **Electronic Digital** Content Store(s) 103 and the Browser 191 on the End-User Device(s) 109. This includes preview of sample **Digital** Content clips. **Digital** Content clips are not packaged into SC(s) but instead are integrated into the **web** service of the **Electronic Digital** Content Store(s) 103 as downloadable files or fed from a streaming server. The format of the Content 113 clip is not dictated by the system architecture. In another embodiment, the Player Application 195 could interact directly with the **Electronic Digital** Content Store(s) 103 or Clearinghouse(s) 105 or offline using a promotional CD.

2. Delivery Over A Computer Readable Medium

In this alternate embodiment, instead of downloading Content 113 or even the Player Application 195 itself over telecommunications lines such as telephone lines, cableTV, direct TV, the **Internet** and other wired and wireless communications infrastructure, in this embodiment a computer readable medium is described. Computer readable medium includes floppy diskettes, CDS, DVDS, Portable... ...from which a computer can read information. For simplicity, in this embodiment, the computer readable medium is a CD 1802 and the Content 113 is **music**. The CD 1802 takes the place of the Content Hosting Sites 111 to permit the **music** to be distributed over physical media rather than through **electronic** means such as broadband. The CD 1802 contains **music** samples and multiple compressed and encrypted **music** tracks in a Content SC 630 and the associated metadata about the Content 113. The sample tracks in the **audio** session can be played back in a standard CD player. When mounted in an CD drive of the End User Device(s) 109 automatically starts a **Web** Browser 191 that allows an end-user to listen to the **music** samples and select one or more of the compressed and encrypted songs for purchase.

The overall buying transaction process is the same as that used... ...read in Content SC(s) 630 stored on CD 1802. Thus, the use of the CD 1802 eliminates the long download times over narrow-band **Internet**, and the need for a broadband **Internet** channel. As previously described, for the telecommunications distribution of Content 113, the end-user using the End User Device(s) 109 access the encryption Key 623 to render the Content 113 by receiving a Transaction SC(s) 641 from the **Electronic Digital** Content Store(s) 103. In an alternative embodiment, the modified Transaction SC(s) 1832 is received from the Content Provider(s) 101, or the ClearingHouse... ...process purchase authorisations.

The number of compressed and encrypted songs that can fit onto CD 1802 depends on the number and playing time of the **music** samples in the **audio** session and on the compressed **music** data rate and the length of each song. For example, if about twenty (20) second **music** samples are allowed, then about four (4) **musical** works of 60-minute length compressed at 256 kilobit/second or eight (8) of 60-minute length albums compressed at 128 kilobit/second will fit... ...If the computer readable medium is a DVD instead of a CD 1802, the current DVD technology stores around 5 times the number of compressed **musical** works over the CD media. Accordingly with current DVD technology it is possible to store twenty (20) 60-minute **musical** works compressed at 256 kilobits/second and forty (40) 60 minute albums compressed at 128 kilobit/second.

One embodiment for the information stored on the... ...information also known as the as the promotional package1801 is broken down into two general areas known : (i) Content Session Area 1804, in this example **audio** content; and (ii) Data Session 1806, which ties into the functionality of the Player Application 195.

Content Session Area 1804 includes:

- An informational **audio** track 1808 with information about the content of the CD 1802 and the procedure to buy one of the included compressed song or songs.

- About 20 30-second **audio** tracks 1820 of promotional **music**.

Data session 1806 includes:

- Autorun.exe 1812 program that launches the data session in the End User Device(s) 109. If the autorun function in... ...of its execution, the autorun.exe 1812 opens the first HTML page of HTML pages 1816 on the CD 1802, which in turn launches the **Web** Browser 191 and the **Web** Browser 191 automatically registers the logical drive identifier from which the first HTML page was opened and uses it as the current reference drive.

- Autorun... ...autorun function in Windows is not enabled. This text file also provides information on the purpose of the CD 1802 and the process to purchase **music**.

- Player Application Installation Package 1818 permits the end-user to install the Player Application 195 on the End User Device(s) 109.

- Set of HTML pages 1816 support navigation of the ed-user to select **music** and gather end-user's credit card information to send to **Electronic Digital** Content Store(s) 103.

- Data set for each compressed album.

- Content SC(s) 630 and associate metadata.

- Offer SC(s) 641 points to the Content... ...Offer SC(s) 641 on the CD 1802, and the available Usage Conditions 519. The modified Transactions SC(s) 1824 maybe digitally signed with a **Digital** Signature 624 of the Content Provider(s) 101.

Turning now to FIG. 19, is a flow diagram of the alternative embodiment of FIG. 18 for acquiring **rights** to **digital** content, according to the present invention. The process begins with the end-user loading the CD 1802 into the End-User Device(s) 109, step 1902. The end-user can listen to the information **audio** track and the **music** samples and other multimedia promotional materials, step 1904. The end-user interacts with the HTML pages read from the CD 1802, the end-user selects the **music** he/she wants to buy and provides credit card information. The HTML pages 1816 presents to the end-user the price and Usage Conditions 519... ...in the telecommunications embodiment.

Once the end-user selects the albums for purchase and provides the credit card information, a browser script program running on **Web** Browser 191 transfers a Notify SC(s) 1822 derived from the CD 1802 and transferred to a payment site such as the **Electronic Digital** Content Store(s) 103, step 1906. A secure connection, such as an SSL connection, is used between the End-User Device(s) 109 and the payment site is used to protect the transfer of the credit card and selection information against eavesdropping in the **Internet**.

After achieving payment authorisation, a modified Transaction SC(s) 1824 is received by the **Web** Browser 191. This modified Transaction SC(s) 1824 is similar to the regular modified Transaction SC(s) 640, but it does not carry the Offer... ...s) 1822. That is, modified Transaction SC(s) 1824 carries Transaction Data 642, the Notify SC(s) 1822 and the Usage Conditions 519 for the **music**, step 1908.

The Play Application 195 receives the Offer SC(s) 641 for the selected **music** from the CD 1802. The application then proceeds with the regular interaction with the Clearinghouse(s) 105 to acquire a **License** SC(s) 660 for the selected Content 113 as describe above in FIG. 6 for the telecommunications embodiment, step 1910.

After a **License** SC(s) 660 for the Content 113 is received, the Player Application 195 copies the corresponding Content SC(s) 630 from the CD 1802, and... ...Content SC(s) 630. If the needed Offer SC(s) 641 are not available on CD 1802 then an HTML address is provided to an **Electronic Digital** Content Store(s) 103.

- Create the Notify SC(s) 1822 composed of identifiers for the corresponding Offer SC(s) 641, the **Digital** Signature 641 and the available Usage Conditions 519.

- Allows the creation of HTML pages that will guide the end-user in the selection and purchase of **music**. The HTML page creation will be based on page templates. The templates should allow the creation and customisation of HTML pages 1816 that can contain information on the **music**. The information about each song can include jacket and cover art, lyrics and usage conditions. The templates allow the creation and customisation of HTML forms... ...points to the first HTML page of the HTML pates 1816 to be presented to the end-user.

- Allows the end-user to select the **audio** information and **music** sample tracks and to point to **online** URLS.

What has been described thus far is content delivery on a CD 1802. It should be noted that the promotional encrypted content on the CD can be part of the regular **music** or DVD CD. The CD 1802 can be created by the process in Sub-section 4. "Decryption 1505, Decompression 1506 and Playback Components 1506" in Section D "The Player Application 195" below. The CD 1802 contains the Promotional Package 1801 from a Content Provider(s) 101 or from the **Electronic Digital** Content Store(s) 103. When this CD 1802 is played, this enables the user or a friend of a user to very quickly purchase **rights** to the Content 113 on CD 1802. In other words, if a user takes a CD 1802 to a friends house to listen to it, the friend can purchase the **rights** to make a copy of the CD 1802 for their own use, without having to download the Content 113 from the Content Hosting Site(s... ...This enables very fast propagation of Promotional Package 1801 between friends and associates. Rather than returning to the store or downloading Content 113 over the **Internet**, the friend can create a copy of the Content 113 encrypted on CD 1802 using the process flow described in FIG. 19 below. Besides the...
...Installation

The Player Application 195 and the Helper Application 1981 are packaged into a self installing executable program which is available for download from many **web** sites or via the embodiment above in the section X.A.3 Delivery Over Computer Readable Medium. The Clearinghouse(s) 105 acts as a central location which hosts the master download page at a public **web** site. It contains links to the locations from which the installation package can be downloaded. The installation package is available at all Content Hosting Site(s) 111 to provide geographic dispersal of the download requests. Each participating **Electronic Digital** Content Store(s) 103 can also make the package available for download from their site or may just provide a link to the master download page at the public **web** site of the Clearinghouse(s) 105.

Any End-User(s) wishing to purchase downloadable Content 113, downloads and install this package. The installation is self... ...package. It unpacks and installs both the Helper Application 198 and the Player Application 195 and also configure the Helper Application 198 to the installed **Web** Browser(s).

As part of the installation, a Public/Private Key 661 pair is created for the End-User Device(s) 109 for use in processing Order and **License** SC(s) 660. A random Symmetric Key (Secret User Key) is also generated for use in protecting song encryption keys in the

License Database 197. The Secret User Key (not shown) is protected by breaking the key into multiple parts and storing pieces of the key in multiple... ...One product this code was introduced is in the IBM ThinkPad 770 laptop computer. Here, the tamper-resistant software was used to protect the DVD **movie** player in the computer. **Digital** Content Provider(s) such as Hollywood studios, concerned about the advent of **digital movies** and the ease at which perfect copies can be made, have insisted that **movies** on DVD disc(s) contain copy protection mechanisms. IBM's tamper-resistant software made it difficult to circumvent these copy protection mechanisms. This is a... ...hackers regarding its true operation. The latter technique is largely ad hoc, but the first two build upon well-known tools in cryptography: encryption and **digital** signatures.

C. Secure Container Processor 192

When the End-User(s) submits the final purchase authorisation to the **Electronic Digital** Content Store(s) 103 for the merchandise he has collected in his shopping cart, his **Web** Browser remains active waiting for a response from the **Web** Server. The **Web** Server at the **Electronic Digital** Content Store(s) 103 processes the purchase and performs the financial settlement and then returns a Transaction SC(s) 640 to the End-User Device(s) 109. The SC(s) Processor 192 (Helper Application 198) is launched by the **Web** Browser to process the SC(s) mime type associated with the Transaction SC(s) 640. FIG. 14 is an example of user interface screens of... ...displayed with this information and the End-User(s) is presented with options to schedule the download(s) of the Content 113 (e.g. for **music**, songs or entire albums), step 1402. The End-User(s) can select immediate download or can schedule the download to occur at a later time... ...at install time. This Order SC(s) 650 is sent via HTTP request to the Clearinghouse(s) 105. When the Clearinghouse(s) 105 returns the **License** SC(s) 660, the Helper Application 198 is re-invoked to process the **License** SC(s) 660. The **License** SC(s) 660 is then opened and the URL of the Content Hosting Site(s) 111 is extracted from the referenced Order SC(s) 650. The **License** SC(s) 660 is then sent to the specified Content Hosting Site 111, via http request through the Browser, requesting download of the Content SC... ...a buffer is filled, it is decrypted using the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the **License** SC(s) 660, which itself is first decrypted using the Private Key. The decrypted buffer is then passed to the watermarking function.

The watermarking 193 extracts the watermarking instructions from the **License** SC(s) 660 and decrypt the instructions using the Private Key of the End-User(s). The watermarking data is then extracted from the **License** SC(s) 660 which includes transaction information such as the purchaser's name as registered with the **Electronic Digital** Content Store(s) 103 from which this Content 113 was purchased or derived from the credit card registration information if the **Electronic Digital** Content Store(s) 103 does not provide a registration function. Also included in the watermark is the purchase date and the Transaction ID 535 assigned by the **Electronic Digital** Content Store(s) 103 to reference the specific records logged for this transaction. The Store Usage Conditions 519 are also included to be used by... ...encrypt the Content 113 using a random

Symmetric Key. Once the download and Decryption and Re-Encryption 194 process is complete, the encryption Key 623 **used** by the **Content** Provider(s) 101 to originally encrypt the Content 113 is now destroyed and the new SEAL key is itself encrypted using the Secret User Key created and hidden at installation time. This new encrypted Seal Key is now stored in the **License** Database 107.

Unlike source performed at the Content Provider(s) 101 and user watermarking performed at the End User Device(s) 109 may need to become an industry standard to be effective. These standards are still evolving. The technology is available to allow control information to be embedded in the **music** and updated a number of times. Until such time as the copy control standards are more stable, alternative methods of copy control have been provided in the Secure **Digital** Content **Electronic** Distribution System 100 so that it does not rely on the copy control watermark in order to provide **rights** management in the consumer device. Storage and p lay/record usage conditions security is implemented utilising encrypted DC Library Collections 196 that are tied to... ...Environment. Software hooks are in place to support copy control watermarking when standards have been adopted. Support exists today for watermarking AAC and other encoded **audio** streams at a variety of compression levels but this technology is still somewhat immature at this time to be put to use as a sole... ...in the selection of the original content encryption algorithm. Thus use of widely accepted and proven industry standard algorithms can be used thus further enhancing **Digital** Content Industry acceptance of the Secure **Digital** Content **Electronic** Distribution System 100.

The second purpose of this Decryption and Re-Encryption 194 process is to remove the requirement that the original master encryption Key 623, **used** by the **Content** Provider(s) 101 to encrypt this Content 113, be stored on every End-User Device(s) 109 which has **licensed** this Content 113. The encrypted master Key 623, as part of the **License** SC(s) 660, is only cached on the hard disk of the End-User Device(s) 109 for a very short time and is in... ...Encryption 194 phase has completed, greatly lessens the possibility of piracy from hackers.

Once the song has been re-encrypted, it is stored in the **Digital** Content Library 196. All metadata required for use by the Player Application 195, is extracted from the associated Offer SC(s) 641 and also stored in the **Digital** Content Library 196, step 1403. Any parts of the metadata which are encrypted, such as the song lyrics, are decrypted and re-encrypted in the same manner as described above for the other content. The same SEAL key used to encrypt the **Content** 113 is **used** for any associated metadata needing to be encrypted.

D. The Player Application 195

1. Overview

The Secure **Digital** Content **Electronic** Distribution Player Application 195 (referred to here as the Player Application 195) is analogous to both a CD, DVD or other **Digital** Content player and to a CD, DVD, or other **digital** content storage management system. At its simplest, it performs Content 113, such as playing songs or videos. At another level, it provides the End- User(s) a tool for managing his/her **Digital** Content Library 196. And just as importantly, it provides for editing and playing of collections of content, such as songs, (referred to here as Play... ...195 is assembled from a collection of components that may be individually selected and customised to the requirements of the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103. A generic version of the player is described, but customisation is possible.

Referring now to FIG. 15 there is shown a... ...sets may be selected, based on the requirements of:

* the platform (Windows, Unix, or equivalent)

* communications protocols (network, cable, etc)

* Content Provider(s) 101 or **Electronic Digital** Content Store(s) 103

* Hardware (CD, DVD, etc)

* Clearinghouse(s) 105 technology and more.

The sections below detail the various component sets. The final section... ...no definitive layout of these components. One such layout is provided in the generic player. Based on requirements from Content Provider(s) 101 and/or **Electronic Digital** Content Store(s) and other requirements, alternate layouts are possible.

This set is...with the components used to present End-User Display 1510 and handle controls called End-User Controls 1511 used for such low-level functions as **audio** playback , and presentation of metadata. Next, the End-User Display Component 1510 is further divided by special function groupings (Play-list, **Digital** Content Library), and then object-container components used for grouping and placing of those lower-level components.

Within the component listings below, any reference to... ...to a CD or other recordable medium only applies to the case where the Player Application 195 has such functionality enabled. Also note that the **term** CD in that context is a generic one, that can also represent various other external recording devices, such as MiniDisc or DVD.

FIG. 16 is... ...performing the Content 113:

* Play/Stop button

* Play button

* Stop button

* Pause button

* Skip forward button

* Skip backward button

* Volume control

* Track position control/display

* **Audio** channel volume level display and more.

Controls for the displaying metadata associated with the Content 113

* Cover Picture button

* Cover Picture object

* Artist Picture button... ...include (corresponding screens of an End-User Interface are shown 1601 - 1605):

Play-list of display container

* Play-list Management button

* Play-list Management window

* **Digital** Content search button

* **Digital** Content search Definition object

* **Digital** Content search Submit button

* **Digital** Content search Results object

* Copy Selected Search Result Item To Play-list button

* Play-list object (editable)

* Play-list Save button

* Play-list Play button

* Play-list Pause button

* Play-list Restart button

* Create CD from Play-list button and more.

Display of **Digital** Content Library 196

* **Digital** content library button

* **Digital** content librarian window

* **Digital** content categories button

* **Digital** content categories object

* By-artist button

* By-genre button

* By-label button

* By-category button

* Delete button

* Add-to-Play-list button

* Copy to CD button

* Song List object

* Song List display container and more

Containers and Misc.

* Player window container

* **Audio** controls container

* Metadata controls container

* Metadata display container

* Toolbar container object

* Sample button

* Download button

* Purchase button

* Record button

* Player Name object

* Label/Provider/Store... ...The use of the Content 113 by the Player Applications 195 on End User Device(s) 109 is logged into a database such as the **License** Database 197. The tracking of each use of Content 113 by the Player Application 195 can be transmitted to one or more logging sites such as the Clearing House(s) 105 or Content Provider(s) 101 or **Electronic Digital** Content Store(s) 103 or any site designated and coupled to Transmission Infrastructures 107. This transmission can be scheduled at predetermined times to upload the... ...example, when duplicating or copying the Content 113 stored at the End User Device(s) 109, on to an external device such as DVD Disc, **digital** tape, flash memory, mini Disc or equivalent read/writeable removable media, the use is updates to the logging site. This may be a precondition to... ...many times the Content 113 was performed; if the Content 113 has been duplicated or copied to an authorised external device such as DVD Disc, **digital** tape or mini-Disc. In cases where there are multiple distinct users of a single Player Application 195 on the End User Device(s) 109... ...any one time and the results extrapolated. In this present embodiment, the actual usage can be measures for the users logging back onto a designated **web** site such as the **Electronic Digital** Content Store(s) 103 or Content Provider(s) 101.

4. Decryption 1505, Decompression 1506 and Playback Components 1506

These components use the keys acquired by the Copy/Play Management components to unlock the **audio** data acquired from the Data Management and Library Access components, apply the appropriate decompression to prepare it for playback, and use system **audio** services to play it. In an alternate embodiment, the **audio** data acquired from the Data Management and Library Access components may be copied to removable media such as CDS, diskettes, tapes or MiniDisks.

5. Data... ...well as handle requests for information about the stored songs.

6. Inter-application Communication Components 1508

These components are used for coordination between the Secure **Digital** Content **Electronic** Distribution Player and other applications (e.g., Browser, helper-app and/or plug-in, etc) that may invoke the Player Application 195, or that the... ...this diagram are required for any player, but may be replaced by specialised versions depending on such things as form of encryption or scrambling being **used**, types of **audio** compression, access methods for the Content 113 library, and more.

Above the Player Object Manager 1501 are Variable Objects 1512, which are mostly derived from... ...the Player Application 195

The following embodiment is for an example where the Player Application 195 running on End-User Device(s) 109 is an **audio** player where Content 113 is **music**. It should be understood to those skilled in the art that other types of Content 113 can be supported by the Player Application 195. A typical **audio** enthusiast has a library of CDS holding songs. All of these are available within the Secure **Digital** Content **Electronic** Distribution System 100. The set of songs that have been purchased from **Electronic Digital** Content Store(s) 103 are stored within a **Digital** Content Library 196 on his or her system. The groupings of songs that are analogous to physical CDS are stored as Play-lists. In some cases a Play-list exactly emulates a CD (e.g., all tracks of a commercially available CD has been purchased from an **Electronic Digital** Content Store(s) 103 as an on-line version of the CD and is defined by a Play-list equivalent to that of the CD). But most Play-lists is put together by End-User(s) to group songs they have stored in the **Digital** Content Libraries on their systems. However for the purposes of the ensuing discussions, an example of a custom made **music** CD is **used** when the **term** a Play- list is mentioned.

When the End-User(s) starts the Player Application 195 explicitly, rather than having it start up via invocation from the SC(s) Processor 192 Application, it pre-loads to the last Play-list that was accessed. If no Play-lists exist in the **Digital** Content Library 196, the Play-list editor is started automatically (unless the user has turned off this feature via a preference setting). See The Play... ...of an End-User Interface 1603):

When the End-User(s) has invoked the Play-list function, these are the available functions:

* Open Play-list

* **Digital** Content Librarian is invoked to display a list of stored Play-lists for selection. Also see **Digital** Content Librarian below for more info.

* Edit Play-list

* Invokes the Play-list Editor (see below), primed with the current Play-list if one has...
...for more info.

* Play-list Info

* Display information about the Play-list.

* Song Info

* Display information about the selected song within the Play-list.

* Visit **web** site

* Load **web** site associated with this Play-list into browser.

* Librarian

* Open the **Digital** Content Librarian window. Also see **Digital** Content Librarian below for more info.

The Play-list Editor (corresponding screen of an End-User Interface 1603):

When invoking the Play-list editor, these are the End-User(s)' options:

* View/Load/Delete Play-lists

* **Digital** Content Librarian is invoked to display a list of stored Play-lists for selection of one to load or delete. Also see **Digital** Content Librarian below for more info.

* Save Play-list

* Current version of Play-list is saved in the **Digital** Content Library 196.

* Delete Song

* Currently selected song is deleted from Play-list.

* Add Song

* **Digital** Content Librarian is invoked in song-search mode, for selection of song to add to the Play-list. Also see **Digital** Content Librarian below for more info.

* Set Song Information

* Display and allow changes to information about the selected song within the play-list. This information is stored within the Play-list, and does not alter information about the song stored within the **Digital** Content Library 196. These things can be changed:

* Displayed Song Title

* End-User(s) notes about the song

* Lead-in delay on playing the song... ...play once, restart when done, etc)

* End-User(s) notes about this Play-list Librarian (corresponding screen of an End-User Interface 1601):

* Open the **Digital** Content Librarian window. Also see **Digital** Content Librarian below for more info.

Song Play

When a song has been prepared for play, either by invoking the Player Application 195 with the song as an argument or by selecting a song for play from a Play-list or within the **Digital** Content Librarian, these are the End-User(s)' options: (corresponding screen of an End-User Interface 1601):

* Play

* Pause

* Stop

* Skip Backward

* Skip Forward

* Adjust Volume

* Adjust Track Position

* View Lyrics

* View Credits

* View CD Cover

* View Artist Picture

* View Track Information

* View other metadata

* Visit **web** site

* Play-list

* Librarian and more.

Digital Content Librarian

The **Digital** Content Librarian can be invoked implicitly when selecting songs or Play-lists (see above) or may be opened in its own window for management of...

18/K/11 (Item 6 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2009 European Patent Office. All rights reserved.

SYSTEMS AND METHODS FOR MATCHING, SELECTING, NARROWCASTING, AND/OR CLASSIFYING BASED ON RIGHTS MANAGEMENT AND/OR OTHER INFORMATION

Country	Number	Kind	Date

Legal Status Type	Pub. Date	Kind	Text

Language

Fulltext Availability Available Text	Language	Update	Word Count
Total Word Count (Document A)			
Total Word Count (Document B)			

Fulltext Availability	Available Text	Language	Update	Word Count
Total Word Count (All Documents)				

Specification: ...B1

The present invention relates to **electronic rights** and transaction management. More particularly, the invention relates to automated systems and methods for efficiently matching, selecting, categorizing and/or classifying and narrowcasting in a distributed **electronic rights** management environment. For example, the invention may provide **electronic** computer based systems and methods for matching, classifying, and/or selecting and narrowcasting **digital** information describing people and/or other things. This matching, classifying, and/or selecting and narrowcasting is based, at least in part, on elements of **rights** management information and one or more other categories of information, wherein such information is used for efficient, trusted event management assuring the execution of one or more controls related to, including, for example, consequences of processing such **digital** information describing people and/or other things.

WO 96/24092 discloses a method and a system for managing a data object so as to comply with predetermined conditions for usage of the data object. To control the usage of the data object, a set of control data, defining **usages** of the data object which comply with the predetermined conditions, is created for the data object. The data object is concatenated with the user set... ...Figures 5-12 and the discussion above provide an introduction to the following detailed description of presently preferred embodiments in accordance with these inventions. The "**electronic** matchmaker" shown in Figures 5-12 is implemented in these more detailed embodiments by a matching and classification utility system 900.

Example Matching And Classification... ...Ginter et al". Such objects may comprise information and/or associated rules for using the information. For example, object classifier 902 may receive as inputs:

rights management information 909 such as rules and/or associated consequences;

things 908 controlled or affected by such **rights** management information including, for example content objects or other information subject to such rules;

items 910 such as metadata, abstracts or the like that describe... ...to classify people. User classifier 904 can classify people based, for example, on:

audit trails 912 indicating how people have used their computers and other **electronic** appliances;

profiles 914 developed by asking users questions about their preferences;

controls 909' that are associated, at least in part, with the user or things... ...909 and/or object descriptors 910;

content 950;

audit trail information 916;

user information such as profiles 914;

class information 952;

user information 954;

other **rights** management information 956;

matching criteria 958;

selection criteria 960; and/or

other information.

Matching and classification utility 900 in this example can provide a variety... ...and or selecting processes;

reports 966 indicating the results of classification, matching, and/or selecting processes;

targeted objects and/or pointers 968;

controls 909;

other **rights** management information; and

other classification, matching and/or selection related information.

A Preferred Embodiment Matching and Classification Utility 900 is a VDE-Aware Commerce Utility... ...a commerce utility system 90 as described in "Shear et al", and may comprise one or more processes securely distributed over one or more secure **electronic** appliances within a "Virtual Distribution Environment" as described in "Ginter et al". Furthermore, the present inventions can be used in combination with and/or make use of a wide array of distributed **electronic** administrative and support services that may be referred to as the "Distributed Commerce Utility." Such a Distributed Commerce Utility may be, among other things, an integrated, modular array of administrative and

support services for **electronic** commerce and **electronic rights** and transaction management. The Distributed Commerce Utility provides, among other advantages, comprehensive, integrated administrative and support services for secure **electronic** commerce and other forms of **electronic** interaction. These administrative and support services can be used to supply a secure foundation for conducting financial management, **rights** management, certificate authority, rules clearing, usage clearing, secure directory services, and other transaction related capabilities functioning over a vast **electronic** network such as the **Internet** and/or over organization internal Intranets, or even in-home networks of **electronic** appliances. Such **electronic** interactions supported by the Distributed Commerce Utility may, for example, entail the broadest range of appliances and distribution media, non-limiting examples of which include... ...ROM and DVD in all their current and future forms.

These administrative and support services can, for example, be adapted to the specific needs of **electronic** commerce value chains in any number of vertical markets, including a wide variety of entertainment applications. **Electronic** commerce participants can, for example, use these administrative and support services to support their interests, and/or they can shape and reuse these services in response to competitive business realities. Non-exhaustive examples of **electronic** commerce participants include individual creators, film and **music** studios, distributors, program aggregators, broadcasters, and cable and satellite operators.

The Distributed Commerce Utility can, for example, make optimally efficient use of commerce administration resources, and can, in at least some embodiments, scale in a practical fashion to optimally accommodate the demands of **electronic** commerce growth. The Distributed Commerce Utility may, for example, comprise a number of Commerce Utility Systems. These Commerce Utility Systems can provide a **web** of infrastructure support available to, and reusable by, the entire **electronic** community and/or many or all of its participants. Different support functions can, for example, be collected together in hierarchical and/or in networked relationships... ...form different Commerce Utility Systems for different design implementations and purposes. These Commerce Utility Systems can, for example, be distributed across a large number of **electronic** appliances with varying degrees of distribution.

Such a "Distributed Commerce Utility" provides numerous additional capabilities and benefits that can be used in conjunction with the particular embodiments shown in the drawings of this application, non-exhaustive examples of which include:

. Enables practical and efficient **electronic** commerce and **rights** management.

. Provides services that securely administer and support **electronic** interactions and consequences.

. Provides infrastructure for **electronic** commerce and other forms of human **electronic** interaction and relationships.

. Optimally applies the efficiencies of modern distributed computing and networking.

. Provides **electronic** automation and distributed processing.

. Supports **electronic** commerce and communications infrastructure that is modular, programmable, distributed and optimally computerized.

. Provides a comprehensive array of capabilities that can be combined to support services that perform various administrative and support roles.

. Maximizes benefits from **electronic** automation and distributed processing to produce optimal allocation and use of resources across a system or network.

. Is efficient, flexible, cost effective, configurable, reusable, modifiable... ...in combination with the inventions disclosed herein.

In more detail, as shown in Figure 14A, matching and classification utility 900 may include one or more **rights** operating system layers 90-1; one or more commerce utility support service layers 90-4; one or more service application connect layers 90-3; and... ...processing environments 154 may be used to support secure functions 90-D. Matching and classification utility 900 may be controlled, at least in part, by **rights** management information such as for example:

VDE-compatible controls 909;

rules and/or their consequences; and/or

other **rights** management information.

Matching and Classification Utility Can Interact With Other Commerce Utility Systems

Figure 15 shows that matching and classification utility 900 can interact and interrelate with other commerce utility systems described in "Shear et al" including for example:

financial clearinghouses 200,

usage clearinghouses 300,

rights and permissions clearinghouses 400,

certifying authorities 500,

secure directory services 600,

transaction authorities 700,

VDE administrators 800, and/or

other commerce utility systems 90.

Figures... ...assignments,

audit information, and/or

other information.

Matching and classification utility 900 may receive from usage clearinghouse 300:

requests for class information,

usage and/or **rights** management information,

audit records, and/or

other information.

Figure 15C shows example interaction between matching and classification utility 900 and **rights** and permissions clearinghouse 400. In this example, **rights** and permissions clearinghouse 400 sends matching and classification authority 900:

controls sets and/or object information;

requests for class information;

clearinghouse usage data; and/or

other information.

In this example, matching and classification utility 900 sends the **rights** and permissions clearinghouse 400:

rights management information such as control sets,

requests for information,

class related information such as classes and/or class assignments, and/or

other information.

Figure 15D... ...utility 900 sends the VDE administrator 800:

requests for administration,

class related information such as classes and/or class assignments,

requests for node and/or **web** information, and/or

other information.

In this example, the VDE administrator 600 sends the matching and classification utility 900:

requests for classification information,

administrative information... ...manufacturing companies in the Pacific rim." Organizations, such as companies, non-profit groups or the like may have their own Commerce Utility Systems 156. Certain **electronic** commerce or other activities (the entertainment industry, for example) might have their own vertically-specialized Commerce Utility Systems 158. Certain geographical, territorial or jurisdictional groups... ...transactions being managed, and a variety of other factors. Delegation of clearing authority may be partial (e.g., delegate usage aggregation but not financial or **rights** management responsibilities), and may be consistent with peer-to-peer processing (e.g., by placing some functions within consumers' **electronic** appliances while keeping some other functions centralized).

Matching and Classification Utilities Can Provide Services to Classes of Nodes, Users, Content Services and/or Transaction Services...4 and 5 might have sub-types as well as types.

A matching and classification utility 900 might break out along content classes (e.g., **movies**; scientific, technical and medical; and software). Subtype A might include first run **movies**, oldies, and art films; subtype B might handle journals and textbooks; and type C might be responsible for games, office, educational content. Peer-to-peer... ...service functions such as for example:

automatic class generation,

automatic matching,

automatic class assignment,

class based searching,

class based directory,

audit by class,

market research,

rights management language processing,

other service functions.

Example Detailed Steps Carried Out By Matching and Classification Utility System 900

The next section of the specification describes... ...categories developed by the classification method that has been applied (Figure 18, block 1849; Figure 19, block 1849'). Finally, the process stores the results in **electronic** and/or non-**electronic** storage in the "write output data" step (Figure 18, block 1850; Figure 19, block 1850').

The "get input data" step 1840, 1840' may involve obtaining attribute and/or parameter data from various sources including, for example:

electronic appliance related attribute data;

user demographic data;

user psychographic data;

available **rights** management rules and/or consequences (e.g., permissions records);

exercised **rights** management rules and/or consequences (e.g., permissions records);

rights management and/or other audit and/or usage records;

any third party source of any information, including **rights** management, usage, audit, statistical, personal, organizational, political, economic, social, religious, business, government, medical, research, academic, literary, military, and/or information and/or data in any... ...process.

Figure 20 shows an example composite record 1852. This composite classification record may contain attributes derived from any or all of a variety of **rights** management and/or other data "harvesting" processes. For example, composite record 1852 may include demographic and/or psychographic data obtained by querying the user 95. It may contain usage data obtained by monitoring audit information produced by various usage transactions. It may contain information reflecting user choices concerning **rights** management information, the **rights** management information available to particular users and/or objects, and **rights** management processes actually performed with respect to particular users and/or particular objects. The information may be analyzed first to

provide statistical and/or other summary information, or individual, more granular information may be provided. The composite record 1852 may also contain attributes of particular **electronic** appliance 100 installations. The particular example composite record 1852 shown in Figure 20 is one non-limiting example composite attribute record containing attributes obtained through... ...travel information, and generally do not participate in "pay per view" events and/or content consumption. Members of class 1 also tend to add new **rights** and/or modify existing **rights** management controls for content, for instance, to add a markup and **redistribute** the **content** in one example, may be less likely to express a religious preference and/or affiliation, and tend to use the **Internet** as an area for "surfing" and exploration.

Members of class 2 tend to pay less for content purchased, seldom travel abroad, tend to be interested in sports, religious content and events, and are more often consumers of **movies** than are members of class 1. Members of class 2 are more likely to "pay per view" than are members of class 1, and are much less likely to add new controls to content and/or modify **rights** acquired. Members of class 2 are more likely to express a religious preference and among those that do, Protestant denominations are more frequently mentioned. Members of class 2 may use the **Internet**, but tend to do so as part of their work role and responsibilities rather than as entertainment, hobbies, and other leisure-time pursuits.

Some methods... ...Appliance Related Data

Figure 24 shows example steps performed by the matching and classification utility 900 to collect appliance attribute data. In this example, an **electronic** appliance 100 may have certain information associated with it. For example, a VDE administrator 800 may initialize appliance 100 with certain information upon appliance installation... ...processing the administrative event(s) using the "create appliance attribute record" method to determine whether the administrator already has the desired information for the particular **electronic** appliance 100. If the operation is successful ("yes" exit to decision block 1512, Figure 24), the VDE administrator 800 may send, to the matching and... ...block 1512, Figure 24), the "create appliance attribute record" method operating at VDE administrator 800 may, in this example, collect the data directly from the **electronic** appliance 100 by sending a VDE container to the appliance, the container containing a "create appliance attribute record" method and one or more associated administrative... ...place) perform block 1516 to send a container 152 with one or more administrative events and the "create appliance attribute record" method directly to the **electronic** appliance 100.

Figures 25(A) and 25(B) together show example steps performed by the "create appliance attribute data" method shown in Figure 24, blocks... ...with the method. This example method (which, as explained above, may be performed by the matching and classification utility 900, the VDE administrator 800, the **electronic** appliance 100, any other **electronic** appliance, or a combination of any or all of these) first locates the site configuration record(s) corresponding to the **electronic** appliance for which appliance attribute data is to be collected (Figure 24A, block 1522). This site configuration

record(s) may, for example, be stored in the **electronic** appliance secure database. The method next locates the permissions record for the site configuration record(s) (Figure 24A, block 1523). The SPE next determines, based... ...audit record (Figure 25A, block 1527).

After completing processing of site configuration records, the method then locates the user configuration record(s) corresponding to the **electronic** appliance for which appliance attribute data is to be collected (Figure 25B, block 1528). This user configuration record(s) may, for example, be stored in the **electronic** appliance secure database. The protected processing environment 154 next locates the permissions record for the user configuration record(s) (Figure 25B, block 1529). The protected... ...events to activate such methods) directly to the user 95 about which demographic information is to be collected (Figure 27B, block 1558). The user's **electronic** appliance 100 may, in response, process the one or more events using the "demographic data query" method, which may write an associated audit record (Figure... ...record (Figure 27B, block 1564, 1566). If the required demographic data is successfully collected ("yes" exit to decision block 1562, Figure 27B), the user's **electronic** appliance may process one or more events using the "create demographic record" method supplied by step 1558, which may write an associated audit record (Figure 27B, block 1568). The **electronic** appliance may then send appropriate administrative events and the demographic attribute record to the matching and classification utility within one or more containers 152 (Figure... ...required data (Figure 30, block 1586). If the required data is available from the repositories ("yes" exit to decision block 1588, Figure 30), then an **electronic** appliance at the repository (in this example) processes one or more events using the "create psychographic attribute record" method supplied by block 1586 in order... ...900 may, in response, send one or more administrative events, a "collect psychographic data" and "create psychographic attribute record" method directly to the user's **electronic** appliance 100 within one or more containers 152 (Figure 30, block 1596). The user's **electronic** appliance 100 may, in turn, process the events using the "collect psychographic data" and "create psychographic attribute record" methods (Figure 30, block 1598, 1600), and... ...and consequences. The matching and classification utility 900 may first send one or more administrative events and a "send permission records" method request to an **electronic** appliance 100 within one or more containers 152 (Figure 33, block 1610). In response, the appliance may process the events using the method, which may...example, information from the permissions record header can be copied into the attribute record (Figure 35A, block 1634), and then the method may locate the **rights** record header (block 1636, Figure 35A). Information from the **rights** record header may be copied into the attribute record (block 1638, Figure 35A), along with the identifier for the corresponding **right**(s) (blocks 1640, 1642, Figure 35A). The process may then recursively locate and harvest data from each method header contained within the **rights** record (blocks 1644, 1646, 1648, Figure 35B). The process may recursively repeat steps 1638-1648 for each **rights** record within the permissions record (as tested for by decision block 1650, Figure 35B). Finally, the entire process of steps 1632-1652 may be performed... ...record 1680-2 shown in Figure 37B includes, as a more detailed example, a user ID number field 1682, an object ID field 1684, a **right** ID field 1686a, a method identifier field 1686b, another **right** ID field 1686c, and corresponding method type fields 1686(d), a further **right** ID field 1686e and

two corresponding method attribute fields 1686f, 1686g, a further **right** ID field 1686h and corresponding method attribute fields 1686i, 1686j.

Figure 37C shows a different example in coding for the Figure 37B example attribute record... ...for assembling rules and consequences. In this example, the matching and classification utility 900 may send one or more administrative events and a "get user **rights** table" method within a container 152 to an **electronic** appliance (Figure 38, block 1690). The **electronic** appliance 100 processes the one or more events using the "get URT" method, which may writes an associated audit record (Figure 38, block 1692). The... ...In this example, the matching and classification utility 900 sends one or more administrative events and a "create attribute record from URT" method to the **electronic** appliance 100 that stores or has access to the user **rights** table information (Figure 39, block 1702). The appliance then processes the events using the method sent to it, and the method writes associated audit information... ...to decision block 1706, Figure 39, block 1708).

Figures 40A, 40B show example steps performed by blocks 1700, 1704 to "create attribute record from user **rights** table." The method begins by checking associated permissions for the user **rights** table records (Figure 40A, block 1720). Assuming that appropriate user and/or group permission is available, the method next locates the user **rights** table (Figure 40A, block 1722), and then begins recursively analyzing the user **rights** table information to harvest desired attribute information from it (Figure 40A, blocks 1724 and following). In this particular example, the method locates the user **rights** table record (block 1724, Figure 40A, and then locates the first **rights** record header within the first user choice record within the URT record (blocks 1726, 1728, Figure 40A). The method copies **rights** record header information to the attribute record (block 1730), and then locates the **right** identifier and copies that to the attribute record (blocks 1732, 1734). The method then recursively locates each method header within the user **rights** table **right** record, and copies corresponding attribute information to the attribute record (blocks 1736, 1738, 1740, Figure 40B). Steps 1728-1740 are performed recursively for each **rights** record within the user choice record (see Figure 40B), decision block 1742), and the above steps are performed recursively for each user choice record within the user **rights** table (see decision block 1744, Figure 40B). Additionally, steps 1724-1744 are performed recursively for each user **rights** table record within the user **rights** table (see Figure 40B, decision block 1746). As a last example step, the method creates a permissions record that controls access and use of the... ...begin by locating a corresponding permissions record (Figure 41, block 1750) and then determining whether there is a permission record corresponding to the corresponding user **rights** table entry (Figure 41, decision block 1752). If there is no such entry ("no" exit to decision block 1752), the method may report failure, write... ...required permissions to enable usage ("yes" exit to decision block 1760, Figure 41), the method may access the permissions record (if any) for the user **rights** table for use in controlling access to the user **rights** table itself (block 1768, Figure 41).

Figures 42A-42C show example **rights** attributes records 1770 that may be obtained from the processes above. The Figure 42A example **rights** attribute record 1770-1 includes a

user or group ID field 1772, an object ID field 1774, and any number of attribute fields 1776(1), ... , 1776(n). The more detailed example **rights** attribute record 1770-2 shown in Figure 42B includes a user ID number field 1772, an object ID field 1774, a **right** ID field 1776a and corresponding method attribute field 1776b, another **right** ID field 1776c and corresponding method attribute field 1776d, a **right** ID field 1776e and corresponding method attribute fields 1776f, 1776g, and another **right** ID field 1776h and corresponding method attribute field 1776i.

Figure 42C shows how the **rights** attribute record 1770 can be encoded numerically as opposed to using characters, as one example.

Example Steps for Assembling Usage Audit Records

Figure 43 shows... ...44 example, the matching and classification utility 900 sends one or more administrative events and a "create attribute record from audit record" method to an **electronic** appliance 100 within one or more containers 152 (Figure 44, block 1792). The appliance 100 may then process the one or more administrative events using... ...1836(1), ... , 1836(n). The more detailed Figure 46B example attribute record 1830-2 includes a user ID number 1832, an object ID 1834, a **right** ID 1836a and associated method characteristic 1836b, another **right** ID 1836c and associated method 1836d and associated statistic 1836e, a further **right** ID 1836f and associated method attribute 1836g, another **right** ID 1836h and associated methods 1836i, 1836j, and associated additional attributes 1836k-1836o. The characteristics shown in fields 1836k-1836o could, for example, be derived... ...and Classification Utility 900 Can Support Narrowcasting or "Push" Distribution Models Based On Classes

Interactions with content, transactions, and other events on the World Wide **Web** are mainly driven today by following chains of hypertext links, using various search engines, and/or indexes, to say nothing of just plain luck and... ...or services. Time consuming and generally inefficient, these search activities share in common the feature that each consumer must intentionally "pull" desired content from a **Web** site to their computer after successfully identifying specific content or services of interest at that time. The present inventions also support "pull" models-a topic... ...VDE node (e.g., a protected processing environment 154) installed on their appliances. These example appliances may be of any kind, including computers, so-called **Web** television or **Web**-TV, DVD appliances with some form of back channel, a settop box with a "back channel", and so on.

Perhaps with the permission of the... ...all or a portion of these audit records in a VDE container 2008 to the matching and classification utility 900. The audit records may contain **rights** management information, including, but not limited to the amount of usage, the amount paid, if any, the payment method used, if any, VDE control sets... ...900 may create at least one object class hierarchy, object class, object classification scheme, object category and/or object category scheme using at least some **rights**

management information and assign at least one object to at least one category and/or class.

The matching and classification utility 900 takes the usage information and other **rights** management information received from the VDE nodes and/or other information sources and may create at least one category and may assign at least one... ...class. In Figure 47, the matching and classification utility 900 sends a VDE container 2002 to content provider 2010 with information showing the classes of **content used** by one or more nodes and/or users along with a request that the provider 2010 send similar content back to one or more users... ...available content that may be of interest to user A given the history of content usage as reflected in VDE audit records and/or other **rights** management information. In this "push" example, classes of content or information about available content may be pushed automatically from (a class of) content providers to... ...at all, for content of interest to them.

In this example, user A receives content that may be most like content the user has already **used**, perhaps like **content used** most frequently in the recent past. The present inventions also support the matching and classification utility 900 and/or content provider sending content that is... ...apparent interests to determine if the user's circle of interest might be a little larger than that indicated by past usage and other, related **rights** management information alone.

In another example, providers may from time to time send content unrelated to the user's apparent interests that may nevertheless reflect... ...900 may, by sending a VDE container with appropriate user and content class information, suggest to a provider that user A receive content similar to **content used** by another member or members in the same group or class as user A. In one example, the matching and classification utility 900 may suggest... ...arrangements may include appliances such as a WebTV interface and/or an intelligent "settop box" connected to an interface device that uses one or more (**digital**) TVs for display. Still other arrangements may include an NC computer without a local hard disk logically connected to at least one server, a personal **digital** assistant with a network connection, and/or any other appliances with suitable processing, storage, and communications capabilities.

Referring again to Figure 47A, each customer appliance... ...as on the same local area network, and/or may be distributed across wide area networks such as multi-location corporate Intranets and/or the **Internet** itself. Among other tasks, messaging services 2058 "listens" for messages destined for that particular appliance or for broadcast messages intended for at least one appliance... ...the US market share of PC vendors, information in text format, costing less than a dollar per item, and for which the subscriber receives the **right** to excerpt at least one whole paragraph, provided that the excerpted amount constitutes less than 25% of the entire item based on word count." This... ...900 may create at least one object class hierarchy, object class, object classification scheme, object category and/or object category scheme using at least some **rights** management information and assign at least one object, item, and/or subscriber to at least one category and/or class.

Subsequent to receipt of the...set of rules and usage consequences that apply to members of one or more item classes, thus potentially improving the efficiency of distribution and of **rights** management. In another example, the rules and content items may be sent in separate VDE containers. In this example, the messaging services 2058 and subject... ...may be installed and run on network routers, network switches, one non-limiting example being ATM switches, and other packet and/or cell switches.

Example: **Digital** Broadcasting Based On Matching And Classification

"Shear et al" discloses a **Digital** Broadcasting Network ("DBN") that may function as a cooperative of **Web** sites and, for example, service providers, with a central and perhaps regional and logical (e.g., market based) headquarters groups, or it may function as... ...fashion in a "higher" level cooperative or corporation.

Figure 48 shows one non-limiting example 2100 of a DBN that includes one or more DBN **Web** servers 2104(1)-2104(n) and one or more **Web** users each with VDE nodes. Users are attracted to a specific DBN server (or servers) because it provides access to specializedcontent and/or services 2108. Based at least in part on **rights** management information 2110 collected from DBN servers, for example, controls associated with the most frequently requested information, the matching and classification utility 900 creates categories... ...The matching and classification utility 900 may create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least DBN server and/or at least some information to at least one category and/or class.

For example, one... ...same. The request may be sent independently of the class information.

In another example, the matching and classification utility 900 may receive content and/or **rights** management information from providers and go on to create classes of content and/or content providers in which the classes may be partly defined using **rights** management data. Content on one class may, among other things, be distinguished from content in another class by price, payment methods, usage opportunities (e.g... ...more specified classes to at least one DBN server.

Non-limiting example Figure 48 shows that the DBN 2100 may consist of video and/or **audio** content providers who send certain categories of video and/or **audio** content 2106 to DBN servers 2104(1) - 2104(n) based on the categories of content each server may specialize in, which, in turn, may be determined at least in part on frequency of usage and/or other **rights** management information sent in VDE containers to the matching and classification utility 900, or to a usage clearinghouse 300 and then to a matching and... ...should send content in specific categories 2106 to specific DBN servers 2104. In turn, each DBN server 2104(1) - 2104(n) delivers video and/or **audio** in VDE containers to

parties interested in such content. In another example, a VDE container may hold both video and **audio** and/or any other content type.

Example: Matching and Classification Utility 900 Can Also Support "Pull" Distribution Models Based On Classes

Notwithstanding the noted trend... ...or node. The classification method may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least one service and/or at least some content to at least one category and/or class.

Subsequently, a VDE... ...These commerce utility systems and servers are also connected to the company Intranet 2418. The company 2406 also maintains one or more connects to the **Internet** 2402. (In another example the company may maintain connections to at least one private network operated by themselves and/or another party in addition to, or instead of one or more connections to the public **Internet**.) The content server(s) may provide access to internal, proprietary company information and/or to external, often commercial information. The internal content server may act... ...2404(A)-2404(C) and/or may host commercial content locally on a content server 2408.

In one example, VDE audit records and/or other **rights** management information are sent in VDE containers 2412 from one or more VDE nodes 2420 to the enterprise usage clearinghouse 300 which may forward at... ...and classification utility 900. The enterprise matching and classification utility 900 may also collect from internal information sources 2414 information in addition to audit and **rights** management information, such as information in a human resources, accounting, and/or budgeting database containing data about company employees. These data may indicate, in one... ...matching and classification utility 900 may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least service and/or at least some content to at least one category and/or class.

In one example, using at least some VDE **rights** management data, for example, whether certain information can be viewed by anyone, by any employee, or only by employees in certain job classes, such as... ...and/or responsibilities.

In turn, the enterprise matching and classification utility 900 sends to at least one external content and/or service provider 2404 on **Internet** 2402 one or more VDE containers 2424 with information that indicates categories of interest. The content providers 2404 may themselves be specialized; in one example... ...of rules and usage consequences that may vary according to class. In this non-limiting example, the class is "content type." The publisher may have **rights** in a wide variety of content and content types. Consequently, the publisher may create rules for text objects that may differ from rules for **audio** objects.

The publisher 2502 sends the class-based rules and usage consequences to a first creator 2504 who also has installed VDE on her or his appliance 2516 and who has also been given one or more certificates and/or other **digital** credentials by the publisher (and/or trusted third party) indicating that he is indeed a creator authorized by the publisher 2502. The publisher has included... ...adds a text file to the container 2520 along with her rules and usage consequences. As before, she also has a certificate and/or other **digital** credential(s) identifying her as authorized by publisher ABC to add and/or modify content and rules and usage consequences. As in the case of... ...and usage consequences to a matching and classification authority 900 who may classify the rules and send the rules and their class assignments to a **rights** and permissions clearinghouse 400. The matching and classification utility 900 may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least one rule to at least one category and/or class.

An authorized first creator 2604 may send a VDE container 2617 to the **rights** and permissions clearinghouse 400 asking for rules in the class "rules for authorized creators, for image objects, from publisher ABC." The **rights** and permissions clearinghouse 400 returns a VDE container 2614 with rules in the requested class. The first creator 2604 uses a packaging application 2616 to package his image using these rules plus rules and usage consequences reflecting his **rights** and wishes and sends the VDE container 2614 to the second creator 2606.

The second creator 2606 also sends a VDE container 2619 to the **rights** and permissions clearinghouse 400 asking for rules and consequences in the class "rules for authorized creators, for text objects, from publisher ABC." The **rights** and permissions clearinghouse 400 returns a VDE container 2621 with rules and consequences in the desired class. The second creator 2606 uses a packaging application... ...individuals, organizations, groups, and/or other classes. Examples of these industries include direct marketing, advertising, yellow and white pages directories, directories of directories, and various **electronic** and paper membership lists and professional directories.

In addition to identifying information such as names, e-mail addresses, physical mailing addresses, phone numbers, fax numbers... ...individuals in class "AF." The requested class could be any class defined by one or more attributes and may be based on usage profilesthat include **rights** management information, non-exhaustive examples of which include price, payment methods accepted, permitted operations, meters, and privacy controls.

The secure directory services 600 returns to... ...interested in certain combinations of leisure-time activities. These classes might have been defined at least in part on the basis of usage and other **rights** management information 2816, for example, the kind of leisure-time information recently looked at, for how long, and/or its cost, and/or the kind of **Web** sites recently frequented, sent from consumer VDE nodes 2802(1)-2802(n) to the matching and classification utility 900, and/or to a usage clearinghouse... ...matching and classification utility 900 may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management

information and assign at least one consumer, service, and/or at least some information to at least one category and/or class.

Example Figure 53 shows that a consumer 2802(1) has recently indicated a preference and/or interest in skiing, **music**, and flying to Colorado. Another consumer 2802(n) has indicated a preference for and/or interest in surfing Hawaii. These preferences may be determined at least in part on the basis of **rights** management information. In response queries sent in one or more VDE containers 2810 from the travel company asking for interest and preference information, the matching... ...may send VDE containers 2806 to the travel company 2801 indicating agreement to buy the package offered or may request additional information or may negotiate **terms** and conditions such as price, departure date, insurance, and the like. These negotiations may be conducted using the inventions described in "Ginter et al", Figures... ...may then send a VDE container 2910 to a matching and classification utility 900 with a query asking who can supply the desired items under **terms** and conditions that are also included in the container. Since these **terms** and conditions may be the subject of negotiations, they may be in a format conducive to VDE-based negotiations as described in "Ginter et al... ...sends at least one VDE container 2918 to buyer A 2904 indicating that they will sell buyer A the previously requested items under the enclosed **terms** and conditions. In another example, there may be some VDE-based (see "Ginter et al", Figures 75A-76B) negotiations between the various parties in this... ...index information, financial performance data for publicly held companies, forecasts, risk management information, options and futures, and the like. The classification method may also utilize **rights** and permissions, including access control information, permitted operations, and/or expiration times and/or dates for **rights** management information. The classification method may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least one element to at least one category and/or class.

In turn, using the VDE aware appliance 3004, the...matching and classification utility 900 may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least some trading information to at least one category and/or class.

The example trader 3102 examines the recommendation and... ...classification authority 900 asking, "which banks are in class A?," where class A are "those banks that offer the highest savings interest, no ATM fees, **online/Web** banking using VDE, insured accounts, free checking with balances larger than $2,500, "image" statements (where check images rather than the actual checks are returned... ...Among the ways in VDE nodes, users, content services, and/or transaction services can be authenticated is through the use of certificates and/or other **digital** credentials issued by an appropriate trusted third party, a certifying authority 500, for instance, that warrants and/or attests to some fact or facts, which... ...authority 900(1-N)s, each of which may provide its services to different classes. where class membership is authenticated using certificates and/or other **digital** credentials. In other examples, additional authentication mechanisms may be used in combination with, or instead of certificates, such as information known only to the

user... ...consequences conditional on class definitions and/or the assignment of members to a class. Class membership may be authenticated by a certificate and/or other **digital** credential issued by one or more commerce participants in addition to, and/or instead of a trusted third party such as a certifying authority 500. For example, a certificate and/or other **digital** credential may attest to user identity, that is, that a user is the user he or she claims to be. Nodes, devices, networks, servers, clients, and services, are other non-limiting examples of other commerce elements that may be authenticated with certificates and/or other **digital** credentials. Any commerce participant may issue a certificate, but other participants are not required to accept a given certificate as an authenticator.

Figure 59 shows... ...In each of these instances, the services of the matching and classification authority 900 may depend upon finding certain authenticating certificate(s) and/or other **digital** credentials on the appropriate VDE nodes.

For example, matching and classification utility 900(1) provides services to nodes 3410(1-n) in the deployment 3402... ...3412 issued by certifying authority 500(1) that provides services to this deployment.

In another example, certifying authority 500(2) provides certificates and/or other **digital** credentials to participants in a higher education value chain3404 consisting of an arbitrary number of colleges and universities 3416(1)-3416(n), providers 3418(1... ...number of users and/or consumers of business information 3422(1)-3422(n), and a certifying authority 500(3) that issues certificates and/or other **digital** credentials to members of the value chain 3406.

In addition to membership in certain deployment, institutional, and/or content usage classes, the matching and classification... ...3428(1)-3428(n) and one or more trading companies 3430(1)-3430(n). In another example, other participants may receive certificates and/or other **digital** credentials, including banks and financial institutions, government authorities, for example, tax and/or customs authorities, consumers, suppliers, and/or transportation companies. The matching and classification... ...a commerce utility system may provide services to more than one class where class membership is indicated by at least one certificate and/or other **digital** credential issued by a certifying authority 500 and/or value chain participant. In one example, matching and classification authority 900 might provide services to the class "Higher Education" and to the class "K-12 Education."

Possession of a certificate and/or other **digital** credential may be among the information used to classify a node, user, appliance, device, entity, and/or other commerce participant, and rules and consequences can... ...one or more authenticated classes and/or on the degree of confidence the rule provider has in the trustedness of the certificate and/or other **digital** credential issuer. In one example, a discount to higher education may be larger if the root for chain of trust for a given certificate is... ...or classes.

Example: Matching And Classification Authority 900 Supports Control Sets Based In Part On Employee Classes, Content Classes, And/Or Certificates And/or Other **Digital** Credentials

Chain of handling and control enables, amongst other things, multiple organizations to work together in secure, trusted, efficient, cooperative commerce processes. One way in... ...the class assignment of individual and/or groups of employees. In part by virtue of their employee classification, at least one employee may receive certain **rights** management information, for example, permission to access certain classes of information or permission to perform one or more permitted operations, transactions and/or events.

Example... ...or other class definitions that apply to employees, members, and/or others associated, affiliated, and/or employed by the organization, group, entity and/or institution. **Rights** management information may be part of the claim definition, for example, permissions to view, modify, excerpt, and so on.

Control sets may provide permissions conditional... ...classes of employees may modify certain information and/or classes of information in a database while others may not. Class membership may be indicated by **digital** credentials, non-limiting examples of which include **digital** certificates and **digital** membership cards. Controls may be conditional on other information as well, for example, some computers and/or display devices may not show certain classes of... ...In another example, this certificate and/or one or more additional certificates may attest to the fact that the insurance company has the appropriate charter, **licenses**, and other grants of authority to be in the health insurance business. The certifying authority 500(1) may also send a certificate in a VDE... ...identity. In another example, this certificate and/or one or more additional certificates may attest to the fact that the hospital has the appropriate charter, **licenses**, and other grants of authority to provide hospital and related services.

The insurance company 3508 may have sent one or more control sets to the... ...information may be treated as members of classes that define permissions, such as "confidential," "secret," "top secret," and so on. Other non-limiting example governmental **rights** may address permissions for import, use, and/or export of certain classes of hard goods, services, currency and financial instruments, and content. Travelers entering the... ...Children, for example, may be prohibited as a matter of law by governments from viewing content in the class "sexually explicit."

Another example of government **rights** is that different tax rules may be applied to different classes of **electronic** commerce transactions using VDE. Example 3700, Figure 62A-62B, shows a certifying authority 500 operated by and/or on behalf of a government issuing a certificate and/or other **digital** credential indicating jurisdiction, namely, country. The certificate is sent in a VDE container 3710(a) to a VDE administrator 800. The government certifying authority 500... ...certificates. The tax class definitions 3712, tax control sets 3714, and government authority certificates 3716' are sent in at least one VDE container to a **rights** and permissions clearinghouse 400, who, in one example, redistributes the tax class definitions 3712(1), tax class control sets 3714(1), and/or

government authorization... ...content of any kind, the appropriate tax control sets 3714(A) are also included in the VDE container. A tax control set is applied whenever **content** is **used** in accordance with a tax class and provided that the appropriate jurisdictional certificate 3710' is present on the VDE node 3706(a). For instance, a... ...The class assigned to each story may be carried in the container as metadata for one or more story objects in another example. An example **Web** browser may request of the information provider an image appropriate to that class, which if available, would be sent in another VDE container.

Class may affect display rules in other example ways as well. For instance, several team sports news stories may be displayed in a **Web** browser window in which a scene from a football or basketball game is faintly discernible in the background. Which image is displayed may be determined certificate and/or other **digital** credential.

A matching and classification utility 900 may send administrative events and/or classification methods 3910 to information providers, one or more other value chain... ...in a VDE container 4006 at least one Uniform Resource Locator (URL) that points to the location of the document(s) on the World Wide **Web**.

The user 4002 in this example sends a message in a VDE container 4008 asking for the document identified in the URL. A provider sends... ...value chain participant, or may have resulted more automatically from the analysis by a matching and classification utility 900 of usage, audit, and/or other **rights** management information and/or of "info exhaust," and/or of preference, demographic, and/or psychographic data and/or classes of data.

In another example, the... ...And/Or Other Object Metadata

Among the numerous advantages of the present inventions is the ability to create classes of classes based in part on **rights** management information. The feature may enhance search efficiency by enabling search engines to locate members of classes provided by any of numerous schemes for object naming and object metadata that have been proposed. For example, the IETF Uniform Resource Locator (URL), the International Standard **Book** Number (ISBN), International Standard Serial Number (ISSN), MARC library catalog records, and the recent proposed "Dublin Core"(Weibel, Stuart, Jean Godby, Eric Miller, and Ron... ...and classification utility 900 which (example step "2") may create new "classes of classes" 4306. These new classes 4306 are then made available on a **Web** page 4308 (example step "3") to interested parties who may then search for objects according to their membership in one (or more) of these new classes of classes. In example step "4" an interested party 4320 sends a VDE container with a request to retrieve the **Web** page 4308 with the classes of metadata information. The **Web** server (in example step "5") returns a copy of the page 4312 to the interested user 4320, who (in example step "6") sends a VDE... ...location information for at least one member of the desired class(es) in the list in container 4316.

Example: Matching and Classification Utility 900 Supports **Electronic** Gambling

Electronic gambling may be among the services that will drive **Internet** growth in coming years. Such services raise many questions for both providers and for users or players of the service. For example, providers want to... ...example, players may be particularly interested in the odds at the game of blackjack. In one example, a player may prefer playing with a single **digital** deck of 52 cards and a particular number of (emulated) shuffles rather than with say four decks and more shuffles, the affect of the latter... ...play may consist of a series of communications in VDE containers between the gambling provider and the gambler.

Example: Matching and classification utility 900 Supports **Electronic** Ticket Sales and Distribution

The performing arts, exhibitions, theaters, and conferences are some non-limiting examples of events that may require tickets for admission. **Electronic** ticket agencies on the **Internet** and other **electronic** arenas provide a connection between the consumer and producers of the event. Consumers may want to know such information as the nature of the event... ...of the ticket purchase at a given price, location, date, event, and/or using a particular payment method.

In another example, the tickets may be **digital** and may have associated with them one or more "seals", **digital** signatures, and/or certificates indicating the authenticity and/or integrity of the **digital** tickets.

While the inventions have been described in connection with what is presently considered to be the most practical and preferred embodiments, the inventions are...

Claims: ...B1

1. A method of securely narrowcasting selected **digital** information to specified recipients, the method comprising:(a) at a receiving appliance (2052), receiving selected **digital** information from a sending appliance (2070) remote from the receiving appliance, the receiving appliance having a secure node (2054) and being associated with a specified recipient;(i) the **digital** information having been selected at least in part based on the **digital** information's membership in a first class; and

      (ii) the specified recipient having been selected at least in part based on membership in a second class; and

(b) the specified recipient using the receiving appliance (2052) to access the received selected **digital** information in accordance with rules and controls associated with the selected **digital** information, the rules and controls being enforced by the receiving appliance secure node (2054),

characterised in that: the first class membership was determined at least in part using **rights** management information;

the second class membership was determined at least in part on the basis of information derived from the specified recipient's creation of, use of, or interaction with **rights** management information;

the selected **digital** information is received in a secure container; and

the rules and controls associated with the selected **digital** information are received in the same secure container as the selected **digital** information.

2. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that includes payment rules and controls information.

3. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that includes audit record information.

4. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that governs saving the associated **digital** information outside a protected environment.

5. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that governs modifying the associated **digital** information.

6. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that governs creating an excerpt of the associated **digital** information.

7. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that governs using the associated **digital** information in the creation of at least one derivative work that incorporates at least part of the **digital** information.

8. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that includes usage and audit information.

9. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that includes membership card information.

10. A method according to claim 1, wherein the first or second class membership is determined at least in part using **rights** management information that includes **digital** certificate information.

11. A method according to claim 1, wherein said received selected **digital** information is at least in part transaction information.

12. A method according to claim 1, wherein said received selected **digital** information is at least in part event information.

13. A method according to claim 1, wherein said received selected **digital** information is at least in part hard goods purchase information.

14. A method according to claim 1, wherein said receiving selected **digital** information is at least in part entertainment information.

15. A method according to claim 14, wherein said entertainment information is at least in part **music** information.

16. A method according to claim 1, wherein said received selected **digital** information is at least in part executable software.

17. A method according to claim 1, wherein said rules and controls at least in part govern... ...at least one value chain rule and control.

19. A method according to claim 1, wherein said rules and controls include governing at least one **right** in a chain of handling and control.

20. A method according to claim 1, wherein said rules and controls at least in part use **digital** certificate information.

21. A method according to claim 1, wherein said rules and controls at least in part use membership card information.

22. A method... ...at least one acceptable clearinghouse is a usage clearinghouse.

28. A method according to claim 25, wherein said at least one acceptable clearinghouse is a **rights** and permissions clearinghouse.

29. A method according to claim 25, wherein said at least one acceptable clearinghouse is a secure directory service.

30. A method... ...personal computer.

43. A method according to claim 1, wherein said receiving appliance is a consumer electronics appliance.

44. A system for securely narrowcasting selected **digital** information to specified recipients, the system comprising:(a) a receiving appliance (2052), for receiving selected **digital** information from a sending appliance (2070) remote from the receiving appliance, the receiving appliance having a secure node (2054) and being associated with a specified recipient; and

> (b) means (900) for selecting the **digital** information at least in part based on the **digital** information's membership in a first class, and for selecting the specified recipient at least in part based on membership in a second class;

> wherein the receiving appliance (2052) is arranged to access the received selected **digital** information in accordance with rules and controls associated with the selected **digital** information, the rules and controls being enforced by the receiving appliance secure node (2054),

characterised in that: the selecting means (900) are arranged to determine
the first class membership at least in part using **rights** management
information, and to determine the second class membership at least in part
on the basis of information derived from the specified recipient's creation
of, use of, or interaction with **rights** management information; and

the receiving appliance (2052) is arranged to receive selected **digital**
information in a secure container, and to receive the rules and controls
associated with the selected **digital** information in the same secure
container as the selected **digital** information.

18/K/12 (Item 7 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS
(c) 2009 European Patent Office. All rights reserved.

Country	Number	Kind	Date			
Legal Status Type				Pub. Date	Kind	Text
...Transfer of **rights** to new applicant...				19		

Language

Fulltext Availability Available Text	Language	Update	Word Count
Total Word Count (Document A)			
Total Word Count (Document B)			
Total Word Count (All Documents)			

Specification: ...distributed content, electronic currency, electronic credit, business
transactions (such as EDI), confidential communications, and the like. VDE can further
be used to enable commercially provided **electronic** content to be made available to users
in user defined portions, rather than constraining the user to use portions of content that
were "predetermined" by a content creator and/or other provider for billing purposes.

VDE, for example, can employ:

1. (1) Secure metering means for budgeting and/or auditing **electronic** content and/or appliance usage;

2. (2) Secure flexible means for enabling compensation and/or billing rates for content and/or appliance usage, including **electronic** credit and/or currency mechanisms for payment means;

3. (3) Secure distributed database means for storing control and usage related information (and employing validated compartmentalization and tagging schemes);

4. (4) Secure **electronic** appliance control means;

5. (5) A distributed, secure, "virtual black box" comprised of nodes located at every user (including VDE content container creators, other content... ...some embodiments, the functions of said hardware element, for certain or all nodes, may be performed by software, for example, in host processing environments of **electronic** appliances;

6. (6) Encryption and decryption means;

7. (7) Secure communications means employing authentication, **digital** signaturing, and encrypted transmissions. The secure subsystems at said user nodes utilize a protocol that establishes and authenticates each node's and/or participant's... ...and content usage; as well as clearinghouse and other administrative and analysis activities employing content usage information.

VDE may be used to migrate most non-**electronic**, traditional information delivery models (including entertainment, reference materials, catalog shopping, etc.) into an adequately secure **digital** distribution and usage management and payment context. The distribution and financial pathways managed by a VDE arrangement may include:

) content creator(s),

) distributor(s),

) redistributor... ...by Host Processing Environments (HPEs)), operate in conjunction with secure communications, systems integration software, and distributed software control information and support structures, to achieve the **electronic** contract/**rights** protection environment of the present invention. Together, these VDE components comprise a secure, virtual, distributed content and/or appliance control, auditing (and other administration), reporting... ...for example, with VDE end-users and content providers. VDE components together comprise a configurable, consistent, secure and "trusted" architecture for distributed, asynchronous control of **electronic** content and/or appliance usage. VDE supports a "universe wide" environment for **electronic** content delivery, broad dissemination, usage reporting, and usage related payment activities.

VDE provides generalized configurability. This results, in part, from decomposition of generalized requirements for supporting **electronic** commerce and data security into a broad range of constituent "atomic" and higher level components (such as load modules, data elements, and methods) that may be variously aggregated together to form control methods for **electronic** commerce applications, commercial **electronic** agreements, and data security arrangements. VDE provides a secure operating environment employing VDE foundation elements along with secure independently deliverable VDE components that enable **electronic** commerce models and relationships to develop. VDE specifically supports the unfolding of distribution models in which content providers, over time, can expressly agree to, or allow, subsequent content providers and/or users to participate in shaping the control information for, and consequences of, use of **electronic** content and/or appliances. A very broad range of the functional attributes important for supporting simple to very complex **electronic** commerce and data security activities are supported by capabilities of the present invention. As a result, VDE supports most types of **electronic** information and/or appliance: usage control (including distribution), security, usage auditing, reporting, other administration, and payment arrangements.

VDE, in its preferred embodiment, employs object software... ...and uses object technology to form "containers" for delivery of information that is (at least in part) encrypted or otherwise secured. These containers may contain **electronic** content products or other **electronic** information and some or all of their associated permissions (control) information. These container objects may be distributed along pathways involving content providers and/or content... ...may be securely moved among nodes of a Virtual Distribution Environment (VDE) arrangement, which nodes operate VDE foundation software and execute control methods to enact **electronic** information usage control and/or administration models. The containers delivered through use of the preferred embodiment of the present invention may be employed both for... ...partially secured.

Content providers who employ the present invention may include, for example, software application and game publishers, database publishers, cable, television, and radio broadcasters, **electronic** shopping vendors, and distributors of information in **electronic** document, **book**, periodical, e-mail and/or other forms. Corporations, government agencies, and/or individual "end-users" who act as storers of, and/or distributors of, **electronic** information, may also be VDE content providers (in a restricted model, a user provides content only to himself and employs VDE to secure his own confidential information against unauthorized use by other parties). **Electronic** information may include proprietary and/or confidential information for personal or internal organization use, as well as information, such as software applications, documents, entertainment materials... ...use of all or portions of communicated information is enforced.

VDE provides important mechanisms for both enforcing commercial agreements and enabling the protection of privacy **rights**. VDE can securely deliver information from one party to another concerning the use of commercially distributed **electronic** content. Even if parties are separated by several "steps" in a chain (pathway) of handling for such content usage information, such information is protected by... ...reporting information

that is then communicated securely to its intended recipient's VDE secure subsystem. Because VDE can deliver such information securely, parties to an **electronic** agreement need not trust the accuracy of commercial usage and/or other information delivered through means other than those under control of VDE.

VDE participants in a commercial value chain can be "commercially" confident (that is, sufficiently confident for commercial purposes) that the direct (constituent) and/or "extended" **electronic** agreements they entered into through the use of VDE can be enforced reliably. These agreements may have both "dynamic" transaction management related aspects, such as content usage control information enforced through budgeting, metering, and/or reporting of **electronic** information and/or appliance use, and/or they may include "static" **electronic** assertions, such as an end-user using the system to assert his or her agreement to pay for services, not to pass to unauthorized parties **electronic** information derived from usage of content or systems, and/or agreeing to observecopyright laws. Not only can electronically reported transaction related information be trusted under... ...a VDE installation in response to control information (located, in the preferred embodiment, in one or more permissions records) stipulating the "withdrawal" of credit or **electronic** currency (such as tokens) from an **electronic** account (for example, an account securely maintained by a user's VDE installation secure subsystem) based upon usage of VDE controlled **electronic content** and/or appliances (such as governments, financial credit providers, and users).

VDE allows the needs of **electronic** commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to...and secured content control information which ensures the performance of control information. Content control information governs content usage according to criteria set by holders of **rights** to an object's contents and/or according to parties who otherwise have **rights** associated with distributing such **content** (such as governments, financial credit providers, and users).

In part, security is enhanced by object methods employed by the present invention because the encryption schemes... ...control information (software control information and relevant data) from modification. Said object techniques also enhance portability between various computer and/or other appliance environments because **electronic** information in the form of content can be inserted along with (for example, in the same object container as) content control information (for said content... ...of participants, and properties of delivered information. A significant feature of VDE accommodates the many, varying distribution and other transaction variables by, in part, decomposing **electronic** commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility... ...and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows **electronic** commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended **electronic** agreement (**electronic** control model). This shaping can occur as content control information passes from one VDE participant to

another and to the extent allowed by "in place... ...recast existing control information and/or add new control information as necessary (including the elimination of no longer required elements).

VDE supports trusted (sufficiently secure) **electronic** information distribution and usage control models for both commercial **electronic** content distribution and data security applications. It can be configured to meet the diverse requirements of a network of interrelated participants that may include content... ...end users, and/or clearinghouses and/or other content usage information users. These parties may constitute a network of participants involved in simple to complex **electronic** content dissemination, usage control, usage reporting, and/or usage payment. Disseminated content may include both originally provided and VDE generated information (such as content usage... ...and content control information handling, as well as the direct usage of content. The configurability provided by the present invention is particularly critical for supporting **electronic** commerce, that is enabling businesses to create relationships and evolve strategies that offer competitive value. **Electronic** commerce tools that are not inherently configurable and interoperable will ultimately fail to produce products (and services) that meet both basic requirements and evolving needs of most commerce applications.

VDE's fundamental configurability will allow a broad range of competitive **electronic** commerce business models to flourish. It allows business models to be shaped to maximize revenues sources, end-user product value, and operating efficiencies. VDE can be employed to support multiple, differing models, take advantage of new revenue opportunities, and deliver product configurations most desired by users. **Electronic** commerce technologies that do not, as the present invention does:

) support a broad range of possible, complementary revenue activities,

) offer a flexible array of content... ...key factors contributing to the configurability intrinsic to the present invention include:

1. (a) integration into the fundamental control environment of a broad range of **electronic** appliances through portable API and programming language tools that efficiently support merging of control and auditing capabilities in nearly any **electronic** appliance environment while maintaining overall system security;

2. (b) modular data structures;

3. (c) generic content model;

4. (d) general modularity and independence of foundation... ...of a pathway of VDE content control information handling.

Because of the breadth of issues resolved by the present invention, it can provide the emerging "**electronic** highway" with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against

unauthorized use of confidential and/or proprietary information and commercial **electronic** transactions. VDE's **electronic** transaction management mechanisms can enforce the **electronic rights** and agreements of all parties participating in widely varying business and data security models, and this can be efficiently achieved through a single VDE implementation within each VDE participant's **electronic** appliance. VDE supports widely varying business and/or data security models that can involve a broad range of participants at various "levels" of VDE content... ...VDE installations and/or users in general; certain specific users, installations, classes and/or other groupings of installations and/or users; as well as to **electronic** content generally on a given installation, to specific properties, property portions, classes and/or other groupings of content.

Distribution using VDE may package both the **electronic** content and control information into the same VDE container, and/or may involve the delivery to an end-user site of different pieces of the... ...user installation. For example, a local VDE installation may perform decryption and save any, or all of, usage metering information related to content and/or **electronic** appliance usage at such user installation could be performed at the server employing secure (e.g., encrypted) communications between said secure subsystems. Said server location... ...said user installation, with, for example, metered information being maintained only temporarily at a local user installation.

Delivery means for VDE managed content may include **electronic** data storage means such as optical disks for delivering one portion of said information and broadcasting and/or telecommunicating means for other portions of said information. **Electronic** data storage means may include magnetic media, optical media, combined magneto-optical systems, flash RAM memory, bubble memory, and/or other memory storage means such... ...to form various VDEF capabilities called control methods and which serve as VDEF applications and operating system functions. When a host operating environment of an **electronic** appliance includes VDEF capabilities, it is called a "**Rights** Operating System" (ROS). VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called "control information." VDEF control information may be specifically associated with one or more pieces of **electronic** content and/or it may be employed as a general component of the operating system capabilities of a VDE installation.

VDEF transaction control elements reflect... ...for example, of VDE templates, to employ specific capabilities, along, for example, with capability parameter data to reflect the elements of one or more express **electronic** agreements between VDE participants in regards to the use of **electronic** content such as commercially distributed products. These control capabilities manage the use of, and/or auditing of use of, **electronic** content, as well as reporting information based upon content use, and any payment for said use. VDEF capabilities may "evolve" to reflect the requirements of... ...of control information. Frequently, for a VDE application for a given content model (such as distribution of entertainment on CD-ROM, content delivery from an **Internet** repository, or **electronic** catalog shopping and advertising, or some combination of the above) participants would be able to securely select from amongst available, alternative control methods and apply... ...Normally the party who creates a VDE content container defines the general

nature of the VDEF capabilities that will and/or may apply to certain **electronic** information. A VDE content container is an object that contains both content (for example, commercially distributed **electronic** information products such as computer software programs, **movies, electronic** publications or reference materials, etc.) and certain control information related to the use of the object's content. A creating party may make a VDE... ...and/or otherwise available for use with, VDE content containers comprise (for commercial content distribution purposes) VDEF control capabilities (and any associated parameter data) for **electronic** content. These capabilities may constitute one or more "proposed" **electronic** agreements (and/or agreement functions available for selection and/or use with parameter data) that manage the use and/or the consequences of use of such content and which can enact the **terms** and conditions of agreements involving multiple parties and their various **rights** and obligations.

A VDE **electronic** agreement may be explicit, through a user interface acceptance by one or more parties, for example by a "junior" party who has received control information from a "senior" party, or it may be a process amongst equal parties who individually assert their agreement. Agreement may also result from an automated **electronic** process during which **terms** and conditions are "evaluated" by certain VDE participant control information that assesses whether certain other **electronic terms** and conditions attached to content and/or submitted by another party are acceptable (do not violate acceptable control information criteria). Such an evaluation process may be quite simple, for example a comparison to ensure compatibility between a portion of, or all senior, control **terms** and conditions in a table of **terms** and conditions and the submitted control information of a subsequent participant in a pathway of content control information handling, or it may be a more... ...adds to and/or otherwise modifies, "in place" content control information, a VDE agreement between two or more parties related to the use of such **electronic** content may be created (so long as any modifications are consistent with senior control information). Acceptance of **terms** and conditions related to certain **electronic** content may be direct and express, or it may be implicit as a result of use of content (depending, for example, on legal requirements, previous exposure to such **terms** and conditions, and requirements of in place control information).

VDEF capabilities may be employed, and a VDE agreement may be entered into, by a plurality of parties without the VDEF capabilities being directly associated with the controlling of certain, specific **electronic** information. For example, certain one or more VDEF capabilities may be present at a VDE installation, and certain VDE agreements may have been entered into during the registration process for a content distribution application, to be **used** by such installation for securely controlling VDE content usage, auditing, reporting and/or payment. Similarly, a specific VDE participant may enter into a VDE user agreement with a VDE content or **electronic** appliance provider when the user and/or her appliance register with such provider as a VDE installation and/or user. In such events, VDEF in... ...that certain VDEF methods are employed, for example in a certain sequence, in order to be able to use all and/or certain classes, of **electronic** content and/or VDE applications.

VDE ensures that certain prerequisites necessary for a given transaction to occur are met. This includes the secure execution of... ...property each time a copy was made for another employee. This same provider might also charge fees based on the total number of different properties **licensed** from them by the user and a metering history of their **licensing** of properties might be required to maintain this information.

VDE provides organization, community, and/or universe wide secure environments whose integrity is assured by processes... ...comprises, at least in part, special purpose circuitry that has been designed to protect against tampering with, or unauthorized observation of, the information and functions **used** in performing the VDE's control functions. The special purpose secure circuitry provided by the present invention includes at least one of: a dedicated semiconductor... ...hardware may be found incorporated into, for example, a fax/modem chip or chip pack, I/O controller, video display controller, and/or other available **digital** processing arrangements. It is anticipated that portions of the present invention's VDE secure hardware capabilities may ultimately be standard design elements of central processing units (CPUs) for computers and various other **electronic** devices.

Designing VDE capabilities into one or more standard microprocessor, microcontroller and/or other **digital** processing components may materially reduce VDE related hardware costs by employing the same hardware resources for both the transaction management uses contemplated by the present invention and for other, host **electronic** appliance functions. This means that a VDE SPU can employ (share) circuitry elements of a "standard" CPU. For example, if a "standard" processor can operate... ...VDE in Accordance With the Present Invention

VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed **electronic** commerce solution. VDE enables an **electronic** commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, VDE includes features that:

"sufficiently" impede unauthorized and/or uncompensated use of **electronic** information and/or appliances through the use of secure communication, storage, and transaction management technologies. VDE supports a model wide, distributed security implementation which creates... ...storage environment. VDE enables distributed VDE installations to securely store and communicate information and remotely control the execution processes and the character of use of **electronic** information at other VDE installations and in a wide variety of ways;

) support low-cost, efficient, and effective security architectures for transaction control, auditing, reporting... ...private key techniques such as triple DES to encrypt content, public key techniques such as RSA to protect communications and to provide the benefits of **digital** signature and authentication to securely bind together the nodes of a VDE arrangement, secure processing of important transaction management executable code, and a combining of... ...preparation (such as causing such content to be placed in a VDE

content container and associating content control information with said content), content and/or **electronic** appliance usage auditing, **content** usage analysis, as well as content usage control; and b) said hardware having been designed to securely handle processing load module control activities, wherein said control processing activities may involve a sequence of required control factors;

) support dynamic user selection of information subsets of a VDE **electronic** information product (VDE controlled **content**). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments such as being required to... ...one or more blocks of a preidentified nature, e.g., bytes, images, logically related blocks) that form a generally arbitrary, but logical to a user, **content** "deliverable." VDE control information (including budgeting, pricing and metering) can be configured so that it can specifically apply, as appropriate, to ad hoc selection of... ...costly than the subset of information needed by the user if such a subset was available. In sum, the present invention allows information contained in **electronic** information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide the greatest value to users, which in turn will generate the greatest amount of **electronic** commerce activity. The user, for example, would be able to define an aggregation of content derived from various portions of an available content product, but... ...and delivery of such portions to the user. VDE further supports a wide variety of predefined increment types including:

) bytes,

) images,

) content over time for **audio** or video, or any other increment that can be identified by content provider data mapping efforts, such as:

) sentences,

) paragraphs,

) articles,

) database records, and

) byte... ...information for security testing in highly secure special purpose VDE installation nonvolatile memory (if available).

) support trusted chain of handling capabilities for pathways of distributed **electronic** information and/or for content usage related information. Such chains may extend, for example, from a content creator, to a distributor, a redistributor, a client... ...independent clearinghouses and then back to the content providers, including content creators. The same and/or different pathways employed for certain content handling, and related **content** control information and reporting information handling, may also be employed

as one or more pathways for **electronic** payment handling (payment is characterized in the present invention as Administrative content) for **electronic** content and/or appliance usage. These pathways are used for conveyance of all or portions of content, and/or content related control information. Content creatorsbased on the timing of past purchases, and

P security budgets based on quantity of different, logically related units of **electronic** information used over an interval of time.Use of bitmap meters (including "regular" and "wide" bitmap meters) to record usage and/or purchase of information... ...conjunction with other elements of the preferred embodiment of the present invention, uniquely supports efficient maintenance of usage history for: (a) rental, (b) flat fee **licensing** or purchase, (c) **licensing** or purchase discounts based upon historical usage variables, and (d) reporting to users in a manner enabling users to determine whether a certain item was... ...certain time period (without requiring the use of conventional database mechanisms, which are highly inefficient for these applications). Bitmap meter methods record activities associated with **electronic** appliances, properties, objects, or portions thereof, and/or administrative activities that are independent of specific properties, objects, etc., performed by a user and/or **electronic** appliance such that a content and/or appliance provider and/or controller of an Administrative activity can determine whether a certain activity has occurred at some point, or during a certain period, in the past (for example, certain use of a commercial **electronic** content product and/or appliance). Such determinations can then be used as part of pricing and/or control strategies of a content and/or appliance... ...launchable" content, that is content that can be provided by a content provider to an end-user, who can then copy or pass along the **content** to other end-user parties without requiring the direct participation of a content provider to register and/or otherwise initialize the content for use. This... ...may be used at some or all VDE installations of a given VDE arrangement since they can make available the content control information necessary for **content** use without requiring the involvement of a commercial VDE value chain participant or data security administrator (e.g. a control officer or network administrator). As... ...VDE installation secure subsystem (such as the presence of a sufficient quantity of financial credit from an authorized credit provider), at least some travelling object **content** may be **used** by a receiving party without the need to establish a connection with a remote VDE authority (until, for example, budgets are exhausted or a time... ...can travel "out-of-channel," allowing, for example, a user to give a copy of a traveling object whose content is a software program, a **movie** or a game, to a neighbor, the neighbor being able to use the traveling object if appropriate credit (e.g. an **electronic** clearinghouse account from a clearinghouse such as VISA or AT&T) is available. Similarly, **electronic** information that is generally available on an **Internet**, or a similar network, repository might be provided in the form of a traveling object that can be downloaded and subsequently copied by the initial... ...or in combination (along with associated data), run as control methods under the VDE transaction operating environment. VDE can satisfy the requirements of widely differing **electronic** commerce and data security applications by, in part, employing this general purpose transaction management foundation to securely process VDE transaction related control methods. Control methods... ...interoperability and/or reliability (e.g., bug control resulting from interaction) between appliances and submitted control methods. The transaction

management control functions of a VDE **electronic** appliance transaction operating environment interact with non-secure transaction management operating system functions to properly direct transaction processes and data related to **electronic** information security, usage control, auditing, and usage reporting. VDE provides the capability to manages resources related to secure VDE content and/or appliance control information execution and data storage.

) facilitate creation of application and/or system functionality under VDE and to facilitate integration into **electronic** appliance environments of load modules and methods created under the present invention. To achieve this, VDE employs an Application Programmer's Interface (API) and/or... ...software's native design. For example, in a VDE aware word processor application, a user may be able to "print" a document into a VDE **content** container object, applying specific control information by selecting from amongst a series of different menu templates for different purposes (for example, a confidential memo template for internal organization purposes may restrict the ability to "keep," that is to make an **electronic** copy of the memo).

) employ "templates" to ease the process of configuring capabilities of the present invention as they relate to specific industries or businesses... ...such as multiple choice, icon selection, and/or prompting for method parameter data (such as identification information, prices, budget limits, dates, periods of time, access **rights** to specific content, etc.) that supply appropriate and/or necessary data for control information purposes. By limiting the typical (non-programming) user to a limited... ...a content or other business model can very substantially limit difficulties associated with content containerization (including placing initial control information on content), distribution, client administration, **electronic** agreement implementation, end-user interaction, and clearinghouse activities, including associated interoperability problems (such as conflicts resulting from security, operating system, and/or certification incompatibilities). Use... ...the template concept may be used to provide individual, overall frameworks for organizations and individuals that create, modify, market, distribute, consume, and/or otherwise use **movies**, **audio** recordings and live performances, magazines, telephony based retail sales, catalogs, computer software, information data bases, multimedia, commercial communications, advertisements, market surveys, infomercials, games, CAD/CAM... ...for user selections or parameter data entry.

) support plural, different control models regulating the use and/or auditing of either the same specific copy of **electronic** information content and/or differently regulating different copies (occurrences) of the same **electronic** information content. Differing models for billing, auditing, and security can be applied to the same piece of **electronic** information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of **electronic** information control increments. This includes supporting variable control information for budgeting and auditing usage as applied to a variety of predefined increments of **electronic** information, including employing a variety of different budgets and/or metering increments for a given **electronic** information deliverable for: billing units of measure, credit limit, security budget limit and security content metering increments, and/or market surveying and

customer profiling content... ...users, other value chain participants (such as clearinghouses and government agencies), and/or user organizations, to specify preferences or requirements related to their use of **electronic** content and/or appliances. Content users, such as end-user customers using commercially distributed content (games, information resources, software programs, etc.), can define, if allowed... ...or other control information, to manage their own internal use of content. Uses include, for example, a user setting a limit on the price for **electronic** documents that the user is willing to pay without prior express user authorization, and the user establishing the character of metering information he or she... ...use of a VDE installation and content and/or appliance usage auditing. In particular, VDE can prevent information related to a participant's usage of **electronic** content from being provided to other parties without the participant's tacit or explicit agreement.

) provide mechanisms that allow control information to "evolve" and be... ...can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, **electronic content** and/or appliances (for example, as related to usage of VDE controlled property content). Independently delivered (from an independent source which is independent except in... ...the overall content control set for a VDE content container is "evolving" as it securely (e.g. communicated in encrypted form and using authentication and **digital** signaturing techniques) passes, at least in part, to a new participant's VDE installation where the proposed control information is securely received and handled. The... ...and said credit account has sufficient credit available. Similarly, control information requiring the payment of taxes and/or the provision of revenue information resulting from **electronic** commerce activities may be securely received by a content provider. This control information may be received, for example, from a government agency. Content providers might... ...multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for concurrent business activities which are dependent on **electronic** commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower... ...or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of **electronic** information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. Alternatively, for example, a one distributor may have the **right** to distribute a different array of properties than another distributor (from a common content collection provided, for example, on optical disc). An individual, and/or... ...from customer use of content and/or appliances, and/or provider and/or end-user payment of taxes, through the transfer of credit and/or **electronic** currency from said end-user and/or provider to a government agency, might occur "automatically" as a result of such received control information causing the... ...to accommodate, under the present invention's preferred embodiment, diverse controlled distributions of VDE controlled content. This allows different parties to employ the same initial **electronic** content with differing (perhaps competitive) control strategies. In this instance, a party who first placed control information on content can make certain control assumptions and...

...model participants submitting control information changes, for example, for use in "negotiating" with "in place" content control information. This can result in new or modified **content** control information and/or it might involve the selection of certain one or more already "i.n-place" content usage control methods over in-place... ...as the submission of relevant control information parameter data. This form of evolution of different control information sets applied to different copies of the same **electronic** property content and/or appliance results from VDE control information flowing "down" through different branches in an overall pathway of handling and control and being... ...ability of the present invention to support multiple pathway branches for the flow of both VDE content control information and VDE managed content enables an **electronic** commerce marketplace which supports diverging, competitive business partnerships, agreements, and evolving overall business models which can employ the same content properties combined, for example, in... ...such that the extracted information is maintained in a continually secure manner through the extraction process. Formation of the new VDE container containing such extracted **content** shall result in control information consistent with, or specified by, the source VDE content container, and/or local VDE installation secure subsystem as appropriate, content... ...specify, for example, who may use at least a portion of the new object, and/or how said at least a portion of said extracted **content** may be **used** (e.g. when at least a portion may be used, or what portion or quantity of portions may be **used**);

(b) allow a user to combine additional content with at least a portion of said extracted content, such as material authored by the extractor and/or content (for example, images, video, **audio**, and/or text) extracted from one or more other VDE container objects for placement directly into the new container;

(c) allow a user to securely... ...encrypted to secure the program).Generally, the extraction features of the present invention allow users to aggregate and/or disseminate and/or otherwise use protected **electronic** content information extracted from content container sources while maintaining secure VDE capabilities thus preserving the **rights** of providers in said content information after various content usage processes.

) support the aggregation of portions of VDE controlled content, such portions being subject to... ...its own control information in the form of one or more permissions records. Alternatively, a negotiation between control information associated with various aggregated portions of **electronic** content, may produce a control information set that would govern some or all of the aggregated content portions. The VDE content control information produced bypotions.

) enable flexible metering of, or other collection of information related to, use of **electronic** content and/or **electronic** appliances. A feature of the present invention enables such flexibility of metering control mechanisms to accommodate a simultaneous, broad array of: (a) different parameters related to **electronic** information content use; (b) different increment units (bytes, documents, properties, paragraphs, images, etc.) and/or other organizations of such **electronic** content; and/or (c) different categories of user and/or VDE installation types, such as client organizations, departments, projects,

networks, and/or individual users, etc... ...or compensation based upon the use and/or exposure to VDE managed content. Such metering is a flexible basis for ensuring payment for content royalties, **licensing**, purchasing, and/or advertising. A feature of the present invention provides for payment means supporting flexible **electronic** currency and credit mechanisms, including the ability to securely maintain audit trails reflecting information related to use of such currency or credit. VDE supports multiple differing hierarchies of client organization control information wherein an organization client administrator distributes control information specifying the usage **rights** of departments, users, and/or projects. Likewise, a department (division) network manager can function as a distributor (budgets, access **rights**, etc.) for department networks, projects, and/or users, etc.

) provide scalable, integratable, standardized control means for use on **electronic** appliances ranging from inexpensive consumer (for example, television set-top appliances) and professional devices (and hand-held PDAs) to servers, mainframes, communication switches, etc. The scalable transaction management/auditing technology of the present invention will result in more efficient and reliable interoperability amongst devices functioning in **electronic** commerce and/or data security environments. As standardized physical containers have become essential to the shipping of physical goods around the world, allowing these physical... ...universally "fit" unloading equipment, efficiently use truck and train space, and accommodate known arrays of objects (for example, boxes) in an efficient manner, so VDE **electronic** content containers may, as provided by the present invention, be able to efficiently move **electronic** information content (such as commercially published properties, **electronic** currency and credit, and content audit information), and associated content control information, around the world. Interoperability is fundamental to efficient **electronic** commerce. The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of **electronic** appliances. The ability, for example, for control methods based on load modules to execute in very "small" and inexpensive secure sub-system environments, such as environments with very little read/write memory, while also being able to execute in large memory sub-systems that may be used in more expensive **electronic** appliances, supports consistency across many machines. This consistent VDE operating environment, including its control structures and container architecture, enables the use of standardized VDE content... ...range of device types and host operating environments. Since VDE capabilities can be seamlessly integrated as extensions, additions, and/or modifications to fundamental capabilities of **electronic** appliances and host operating systems, VDE containers, **content** control information, and the VDE foundation will be able to work with many device types and these device types will be able to consistently and... ...this integration users can also benefit from a transparent interaction with many of the capabilities of VDE. VDE integration with software operating on a host **electronic** appliance supports a variety of capabilities that would be unavailable or less secure without such integration. Through integration with one or more device applications and/or device operating environments, many capabilities of the present invention can be presented as inherent capabilities of a given **electronic** appliance, operating system, or appliance application. For example, features of the present invention include: (a) VDE

system software to in part extend and/or modify host operating systems such that they possesses VDE capabilities, such as enabling secure transaction processing and **electronic** information storage; (b) one or more application programs that in part represent tools associated with VDE operation; and/or (c) code to be integrated into... ...to integrate VDE capabilities and makes such applications VDE aware (for example, word processors, database retrieval applications, spreadsheets, multimedia presentation authoring tools, film editing software, **music** editing software such as MIDI applications and the like, robotics control systems such as those associated with CAD/CAM environments and NCM software and the like, **electronic** mail systems, teleconferencing software, and other data authoring, creating, handling, and/or usage applications including combinations of the above). These one or more features (which... ...may be employed in conjunction with a VDE node secure hardware processing capability, such as a microcontroller(s), microprocessor(s), other CPU(s) or other **digital** processing logic.

) employ audit reconciliation and usage pattern evaluation processes that assess, through certain, normally network based, transaction processing reconciliation and threshold checking activities, whether... ...arrangement have occurred. These processes are performed remote to VDE controlled content end-user VDE locations by assessing, for example, purchases, and/or requests, for **electronic** properties by a given VDE installation. Applications for such reconciliation activities include assessing whether the quantity of remotely delivered VDE controlled content corresponds to the amount of financial credit and/or **electronic** currency employed for the use of such content. A trusted organization can acquire information from content providers concerning the cost for content provided to a given VDE installation and/or user and compare this cost for content with the credit and/or **electronic** currency disbursements for that installation and/or user. Inconsistencies in the amount of content delivered versus the amount of disbursement can prove, and/or indicate... ...be useful in determining whether security at such one or more installations, and/or by such one or more users, has been compromised, particularly when **used** in combination with an assessment of **electronic** credit and/or currency provided to one or more VDE users and/or installations, by some or all of their credit and/or currency suppliers... ...administration and control, security management, user interfaces, payment disbursement, and clearinghouse related functions. These components are designed to support highly secure, uniform, consistent, and standardized: **electronic** commerce and/or data security pathway(s) of handling, reporting, and/or payment; content control and administration; and human factors (e.g. user interfaces).

) support... ...arrangement, including usage information analysis, and control of VDE activities by individuals and groups of employees such as specifying budgets and the character of usage **rights** available under VDE for certain groups of and/or individual, client personnel, subject to control information series to control information submitted by the client administrator... ...database processing means). A financial clearinghouse normally receives at its location securely delivered content usage information, and user requests (such as requests for further credit, **electronic** currency, and/or higher credit limit). Reporting of usage information and user requests can be used for supporting **electronic** currency, billing, payment and credit related activities, and/or for user profile analysis and/or broader market survey analysis and marketing (consolidated) list

generation or... ...secure subsystems. Clearinghouse processing means would normally be connected to specialized I/O means, which may include high speed telecommunication switching means that may be **used** for secure communications between a clearinghouse and other VDE pathway participants.

) securely support **electronic** currency and credit usage control, storage, and communication at, and between, VDE installations. VDE further supports automated passing of **electronic** currency and/or credit information, including payment tokens (such as in the form of **electronic** currency or credit) or other payment information, through a pathway of payment, which said pathway may or may not be the same as a pathway... ...payment may be placed into a VDE container created automatically by a VDE installation in response to control information stipulating the "withdrawal" of credit or **electronic** currency from an **electronic** credit or currency account based upon an amount owed resulting from usage of VDE controlled **electronic** content and/or appliances. Payment credit or currency may then be automatically communicated in protected (at least in part encrypted) form through telecommunication of a... ...conditionally" to fully anonymous currency) and/or further can regulate certain content information, such as currency and/or credit use related information (and/or other **electronic** information usage data) to be available only under certain strict circumstances, such as a court order (which may itself require authorization through the use of... ...in VDE container content and/or control information, potential copyright violators may be deterred from unauthorized extraction or copying. Fingerprinting normally is embedded into unencrypted **electronic** content or control information, though it can be embedded into encrypted content and later placed in unencrypted content in a secure VDE installation sub-system as the encrypted content carrying the fingerprinting information is decrypted. **Electronic** information, such as the content of a VDE container, may be fingerprinted as it leaves a network (such as **Internet**) location bound for a receiving party. Such repository information may be maintained in unencrypted form prior to communication and be encrypted as it leaves the... ...be re-encrypted for transmission. Embedding identification information of the intended recipient user and/or VDE installation into content as it leaves, for example, an **Internet** repository, would provide important information that would identify or assist in identifying any party that managed to compromise the security of a VDE installation or... ...VDE installation. Such hidden information will act as a strong disincentive that should dissuade a substantial portion of potential content "pirates" from stealing other parties **electronic** information. Fingerprint information identifying a receiving party and/or VDE installation can be embedded into a VDE object before, or during, decryption, replication, or communication of VDE content objects to receivers. Fingerprinting **electronic** content before it is encrypted for transfer to a customer or other user provides information that can be very useful for identifying who received certain... ...in unencrypted form. This information would be useful in tracking who may have "broken" the security of a VDE installation and was illegally making certain **electronic** content available to others.

Fingerprinting may provide additional, available information such as time and/or date of the release (for example extraction) of said content... ...incorporated into a property by modifying in a normally undetectable way color frequency and/or the brightness of certain image pixels, by slightly modifying certain **audio** signals as to frequency, by modifying font character formation, etc. Fingerprint information, itself, should be encrypted so as to make it particularly difficult for tampered... ...budgets, authorizations, credit or currency, and content. For example, smart objects may travel to and/or from remote information resource locations and fulfill requests for **electronic** information content. Smart objects can, for example, be transmitted to a remote location to perform a specified database search on behalf of a user or... ...of remote resources (e.g. centralized databases, super computers, etc.) while providing a secure means for charging users based on information and/or resources actually **used**.

) support both "translations" of VDE **electronic** agreements elements into modern language printed agreement elements (such as English language agreements) and translations of **electronic rights** protection/transaction management modern language agreement elements to **electronic** VDE agreement elements. This feature requires maintaining a library of textual language that corresponds to VDE load modules and/or methods and/or component assemblies. As VDE methods are proposed and/or employed for VDE agreements, a listing of textual **terms** and conditions can be produced by a VDE user application which, in a preferred embodiment, provides phrases, sentences and/or paragraphs that have been stored... ...legal, binding agreement), would review the generated document material upon completion and employ such additional textual information and/or editing as necessary to describe non **electronic** transaction elements of the agreement and make any other improvements that may be necessary. These features further support employing modern language tools that allow one or more users to make selections from choices and provide answers to questions and to produce a VDE **electronic** agreement from such a process. This process can be interactive and the VDE agreement formulation process may employ artificial intelligence expert system technology that learns from responses and, where appropriate and based at least in part on said responses, provides further choices and/or questions which "evolves" the desired VDE **electronic** agreement.

) support the use of multiple VDE secure subsystems in a single VDE installation. Various security and/or performance advantages may be realized by employing a distributed VDE design within a single VDE installation. For example, designing a hardware based VDE secure subsystem into an **electronic** appliance VDE display device, and designing said subsystem's integration with said display device so that it is as close as possible to the point... ...to prepare and telecommunicate to said content provider both content usage based information in a certain form, and content usage payment in the form of **electronic** credit (such credit might be "owned" by the provider after receipt and used in lieu of the availability or adequacy of **electronic** currency) and/or **electronic** currency. This delivery of information and payment may employ trusted VDE installation secure subsystems to securely, and in some embodiments, automatically, provide in the manner... ...ensure that a requirement that a clearinghouse report such usage information and payment content will be observed. For example, if one participant to a VDE

electronic agreement fails to observe such information reporting and/or paying obligation, another participant can stop the delinquent party from successfully participating in VDE activities related... ...a similar impact as failing to refresh budgets or time-aged authorizations.

) support smart card implementations of the present invention in the form of portable **electronic** appliances, including cards that can be employed as secure credit, banking, and/or money cards. A feature of the present invention is the use of... ...cards at retail and other establishments, wherein such cards can "dock" with an establishment terminal that has a VDE secure sub-system and/or an **online** connection to a VDE secure and/or otherwise secure and compatible subsystem, such as a "trusted" financial clearinghouse (e.g., VISA, Mastercard). The VDE card and the terminal (and/or **online** connection) can securely exchange information related to a transaction, with credit and/or **electronic** currency being transferred to a merchant and/or clearinghouse and transaction information flowing back to the card. Such a card can be used for transaction activities of all sorts. A docking station, such as a PCMCIA connector on an **electronic** appliance, such as a personal computer, can receive a consumer's VDE card at home. Such a station/card combination can be used for on-line transactions in the same manner as a VDE installation that is permanently installed in such an **electronic** appliance. The card can be used as an "**electronic** wallet" and contain **electronic** currency as well as credit provided by a clearinghouse. The card can act as a convergence point for financial activities of a consumer regarding many... ...paycheck and/or investment earnings and/or "authentic" VDE content container secured detailed information on such receipts, through on-line connections. A user can send **digital** currency to another party with a VDE arrangement, including giving away such currency. A VDE card can retain details of transactions in a highly secure... ...that financially related information is both consolidated and very easily retrieved and/or analyzed. Because of the VDE security, including use of effective encryption, authentication, **digital** signaturing, and secure database structures, the records contained within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements. In some embodiments of the present invention a VDE card may employ docking station and/or **electronic** appliance storage means and/or share other VDE arrangement means local to said appliance and/or available across a network, to augment the information storage... ...authentic" information securely stored and available to said VDE card. Said information may be stored in said card, in said docking station, in an associated **electronic** appliance, and/or other device operatively attached thereto, and/or remotely, such as at a remote server site. A card's data, e.g. transaction history, can be backed up to an individual's personal computer or other **electronic** appliance and such an appliance may have an integrated VDE installation of its own. A current transaction, recent transactions (for redundancy), or all or other... ...current transaction during a connection with another party's VDE installation (for example a VDE installation that is also on a financial or general purpose **electronic** network), by posting transaction information to a remote clearinghouse and/or bank, can ensure that sufficient backup is conducted to enable complete reconstruction of VDE... ...flexible content distribution models.

) support, complete, modular separation of the control structures related to (1) content event triggering, (2) auditing, (3) budgeting (including specifying no **right** of use or unlimited **right** of use), (4) billing, and (5) user identity (VDE installation, client name, department, network, and/or user, etc.). The independence of these VDE control structures...if allowed by senior control information), collect audit information reflecting usage of database fields by different individuals and client organization departments and ensure that differing **rights** of access and differing budgets limiting database usage can be applied to these client individuals and groups. Enabling content providers and users to practically employ... ...the use of such independent control capabilities. As a result, VDE can support great configurability in creation of plural control models applied to the same **electronic** property and the same and/or plural control models applied to differing or entirely different content models (for example, home banking versus **electronic** shopping).

Methods, Other Control Information, and VDE Objects

VDE control information (e.g., methods) that collectively control use of VDE managed properties (database, document, individual... ...end-users from electronically saving decrypted content, a provider of credit for VDE transactions might require an audit method that records the time of an **electronic** purchase, and/or a user might require a method that summarizes usage information for reporting to a clearinghouse (e.g. billing information) in a way... ...can select from among a set of predefined methods (if available) to control container content usage and distribution functions and/or they may have the **right** to provide new customized methods to control at least certain usage functions (such "new" methods may be required to be certified for trustedness and interoperability... ...administrator's control information, which may take precedence over an end-user's control information. A path of distribution participant's ability to set such **electronic** content control information can be limited to certain control information (for example, method mediating data such as pricing and/or sales dates) or it may... ...pathway participants, and/or (b) comprise control information put in place by such a participant on behalf of a party who does not directly handle **electronic** content (or **electronic** appliance) permissions records information (for example control information inserted by a participant on behalf of a financial clearinghouse or government agency). Such control information methods (and/or load modules and/or mediating data and/or component assemblies) may also be put in place by either an **electronic** automated, or a semi-automated and human assisted, control information (control set) negotiating process that assesses whether the use of one or more pieces of... ...and how such control information may be used.

Control information may be provided by a party who does not directly participate in the handling of **electronic** content (and/or appliance) and/or control information for such content (and/or appliance). Such control information may be provided in secure form using VDE... ...secure subsystems, and a pathway of VDE content control information participant's VDE installation secure subsystem. This control information may relate to,

for example, the **right** to access credit supplied by a financial services provider, the enforcement of regulations or laws enacted by a government agency, or the requirements of a... ...or manner of reporting of usage information received by such customer. Such control information may, for example, enforce societal requirements such as laws related to **electronic** commerce.

VDE content control information may apply differently to different pathway of content and/or control information handling participants. Furthermore, permissions records **rights** may be added, altered, and/or removed by a VDE participant if they are allowed to take such action. **Rights** of VDE participants may be defined in relation to specific parties and/or categories of parties and/or other groups of parties in a chain... ...party or parties, may be limited in the number of modifications, and/or degree of modification, they may make.

At least one secure subsystem in **electronic** appliances of creators, distributors, auditors, clearinghouses, client administrators, and end-users (understanding that two or more of the above classifications may describe a single user... ...Storing control and metering related information;

3. 3. Managing communications;

4. 4. Processing core control programs, along with associated data, that constitute control information for **electronic** content and/or appliance **rights** protection, including the enforcing of preferences and requirements of VDE participants.

Normally, most usage, audit, reporting, payment, and distribution control methods are themselves at least... ...e.g. encrypted and authenticated) communications when passing information between the participant location (nodes) secure subsystems of a VDE arrangement, important components of a VDE **electronic** agreement can be reliably enforced with sufficient security (sufficiently trusted) for the intended commercial purposes. A VDE **electronic** agreement for a value chain can be composed, at least in part, of one or more subagreements between one or more subsets of the value chain participants. These subagreements are comprised of one or more **electronic** contract "compliance" elements (methods including associated parameter data) that ensure the protection of the **rights** of VDE participants.

The degree of trustedness of a VDE arrangement will be primarily based on whether hardware SPUs are employed at participant location secure... ...within the security limitations of a given VDE security implementation design). This control information can determine, for example:

1. (1) How and/or to whom **electronic** content can be provided, for example, how an **electronic** property can be distributed;

2. (2) How one or more objects and/or properties, or portions of an object or property, can be directly used... ...which negotiation establishes what control information shall

constitute the resulting control information set for a given piece of VDE managed content and/or VDE installation.

Electronic Agreements and **Rights** Protection

An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and **rights** protection for, **electronic** agreements implemented through the use of the present invention. Such agreements may involve one or more of:

1. (1) creators, publishers, and other distributors, of **electronic** information,

2. (2) financial service (e.g. credit) providers,

3. (3) users of (other than financial service providers) information arising from content usage such as... ...and government agencies,

4. (4) end users of content,

5. (5) infrastructure service and device providers such as telecommunication companies and hardware manufacturers (semiconductor and **electronic** appliance and/or other computer system manufacturers) who receive compensation based upon the use of their services and/or devices, and

6. (6) certain parties described by **electronic** information.

VDE supports commercially secure "extended" value chain **electronic** agreements. VDE can be configured to support the various underlying agreements between parties that comprise this extended agreement. These agreements can define important **electronic** commerce considerations including:

1. (1) security,

2. (2) content use control, including **electronic** distribution,

3. (3) privacy (regarding, for example, information concerning parties described by medical, credit, tax, personal, and/or of other forms of confidential information),

4. (4) management of financial processes, and

5. (5) pathways of handling for **electronic** content, content and/or appliance control information, **electronic** content and/or appliance usage information and payment and/or credit.

VDE agreements may define the **electronic** commerce relationship of two or more parties of a value chain, but such agreements may, at times, not directly obligate or otherwise directly involve other VDE value chain participants. For example, an **electronic** agreement between a content creator and a distributor may establish both the price to the distributor for a creator's content (such as for a... ...end-user agrees to certain requirements for using the distributed product such as accepting distributor charges for content use and agreeing to observe the copyright **rights** of the creator. A third agreement might exist between the distributor and a financial clearinghouse that allows the distributor to employ the clearinghouse's credit... ...evolving agreement may develop between all value chain participants as content control information passes along its chain of handling. This evolving agreement can establish the **rights** of all parties to content usage information, including, for example, the nature of information to be received by each party and the pathway of handling... ...In the above example, these six agreements could comprise agreements of an extended agreement for this commercial value chain instance.

VDE agreements support evolving ("living") **electronic** agreement arrangements that can be modified by current and/or new participants through very simple to sophisticated "negotiations" between newly proposed content control information interacting... ...three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer).

Electronic agreements supported by the preferred embodiment of the present invention can vary from very simple to very elaborate. They can support widely diverse information management models that provide for **electronic** information security, usage administration, and communication and may support:

1. (a) secure **electronic** distribution of information, for example commercial literary properties,

2. (b) secure **electronic** information usage monitoring and reporting,

3. (c) secure financial transaction capabilities related to both **electronic** information and/or appliance usage and other **electronic** credit and/or currency usage and administration capabilities,

4. (d) privacy protection for usage information a user does not wish to release, and

5. (e) "living" **electronic** information content dissemination models that flexibly accommodate:

1. (1) a breadth of participants,

2. (2) one or more pathways (chains) for: the handling of content, content and/or appliance control information, reporting of content and/or appliance usage related information, and/or payment,

3. (3) supporting an evolution of **terms** and conditions incorporated into content control information, including use of **electronic** negotiation capabilities,

4. (4) support the combination of multiple pieces of content to form new content aggregations, and

5. (5) multiple concurrent models.

Secure Processing... ...invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other **electronic** appliance, or network. SPUs provide a trusted environment for generating decryption keys, encrypting and decrypting information, managing the secure communication of keys and other information between **electronic** appliances (i.e. between VDE installations and/or between plural VDE instances within a single VDE installation), securely accumulating and managing audit trail, reporting, and... ...of certain control software, one or more tamper resistant hardware modules such as a semiconductor or semiconductor chipset (including, for example, a tamper resistant hardware **electronic** appliance peripheral device), for use within, and/or operatively connected to, an **electronic** appliance. With the present invention, the trustedness of a hardware SPU can be enhanced by enclosing some or all of its hardware elements within tamper... ...VDE processes.

A VDE node's hardware SPU is a core component of a VDE secure subsystem and may employ some or all of an **electronic** appliance's primary control logic, such as a microcontroller, microcomputer or other CPU arrangement. This primary control logic may be otherwise employed for non VDE purposes such as the control of some or all of an **electronic** appliance's non-VDE functions. When operating in a hardware SPU mode, said primary control logic must be sufficiently secure so as to protect and conceal important VDE processes. For example, a hardware SPU may employ a host **electronic** appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security... ...connects to communications means 202 such as telephone or cable TV lines for example. Telephone or cable TV lines 202 may be part of an "**electronic** highway" that carries **electronic** information from place to place. Lines 202 connect information utility 200 to other people such as for example a consumer 208, an office 210, a... ...virtual distribution environment 100. A few of many examples of transactions that can be supported by virtual distribution environment 100 include:

C home banking and **electronic** payments;

C **electronic** legal contracts;

C distribution of "content" such as **electronic** printed matter, video, **audio**, images and computer programs; and

C secure communication of private information such as medical records and financial information.

Virtual distribution environment 100 is "virtual" because it does not require many of the physical "things" that used to be necessary to protect **rights**, ensure reliable and predictable distribution, and ensure proper compensation to content creators and distributors. For example, in the past, information was distributed on records or... ...goods and services only after they handed cash over to a seller. Although information utility 200 may deliver information by transferring physical "things" such as **electronic** storage media, the virtual distribution environment 100 facilitates a completely **electronic** "chain of handling and control."

VDE Flexibility Supports Transactions

Information utility 200 flexibly supports many different kinds of information transactions. Different VDE participants may define... ...with delivering information about a transaction, or it may be one of the transaction participants.

For example, the video production studio 204 in the upper **right**-hand corner of Figure 1 may create video/television programs. Video production studio 204 may send these programs over lines 202... ...the video production studio or information utility 200 has arranged for these consumers to have appropriate "rules and controls" (control information) that give the consumers **rights** to use the programs.

Even if a consumer has a copy of a video program, she cannot watch or copy the program unless she has... ...FIGREF> also shows a publishing house 214. Publishing house 214 may act as a distributor for an author 206. The publishing house 214 may distribute **rights** to use "content" (such as computer software, **electronic** newspapers, the video produced by publishing house 214, **audio**, or any other data) to consumers such as office 210. The use **rights** may be defined by "rules and controls" distributed by publishing house 216. Publishing house 216 may distribute these "rules and controls" with the content, but this is not necessary. Because the **content** can be **used** only by consumers that have the appropriate "rules and controls," content and its associated "rules and controls" may be distributed at different times, in different... ...VDE participants. The ability of VDE to securely distribute and enforce "rules and controls" separately from the content they apply to provides great advantages.

Use **rights** distributed by publishing house 214 may, for example, permit office 210 to make and distribute copies of the content to its employees. Office 210 may... ...permit only specified employees and/or groups to access certain information.

Figure 1 also shows an information delivery service 216 delivering **electronic** storage media such as "CD ROM" disks to consumers 206. Even though the **electronic** storage media themselves are not delivered electronically by information utility 200 over lines

202, virtual distribution environment 100. The **electronic** storage media may be **used** to distribute **content**, "rules and controls," or other information.

Example of What's Inside Information Utility 200

"Information utility" 200 in Figure 1 can... ...utility participants 200a-200g could each be an independent organization/business. There can be any number of each of participants 200a-200g. In this example, **electronic** "switch" 200a connects internal parts of information utility 200 to each other and to outside participants, and may also connect outside participants to one another.

Information utility 200 may include a "transaction processor" 200b that processes transactions (to transfer **electronic** funds, for example) based on requests from participants and/or report receiver 200e. It may also include a "usage analyst" 200c that analyzes reported usage... ...102 may also specify "rules and controls" for distributing the content. These distribution-related "rules and controls" can specify who has permission to distribute the **rights** to use content, and how many users are allowed to use the content.

Arrow 104 shows the content creator 102 sending the "rules and controls" associated with the content to a VDE **rights** distributor 106 ("distributor") over an **electronic** highway 108 (or by some other path such as an optical disk sent by a delivery service such as U. S. mail). The content can... ...usage-related "rules and controls" must be consistent with the "rules and controls" specified by content creator 102.

Arrow 110 shows the distributor 106 distributing **rights** to use the content by sending the content's "rules and controls" to a content user 112 such as a consumer. The content user 112... ...done differently. For example, clearinghouse 116 may directly or through an agent, provide reports and/or payments to each of VDE content creators 102, and **rights** distributor 106, as well as reports to content user 112.

The distributor 106 and the content creator 102 may be the same person, or they may be Different people. For example, a **musical** performing group may act as both content creator 102 and distributor 106 by creating and distributing its own **musical** recordings. As another example, a publishing house may act as a distributor 106 to distribute **rights** to use works created by an author content creator 102. Content creators 102 may use a distributor 106 to efficiently manage the financial end of... ...content creator 102.

Every VDE participant in "chain of handling and control" is normally subject to "rules and controls." "Rules and controls" define the respective **rights** and obligations of each of the various VDE participants. "Rules and controls" provide information and mechanisms that may establish interdependencies and relationships between the participants... ...appropriate permission, if required. This ability to securely control what information is revealed and what VDE participant(s) it is revealed to allows the privacy **rights** of all VDE participants to be protected.

Rules and Contents" Can Be Separately Delivered

As mentioned above, virtual distribution environment 100 "associates" content with corresponding "rules and controls," and prevents the **content** from being **used** or accessed unless a set of corresponding "rules and controls" is available. The distributor 106 doesn't need to deliver content to control the content... ...content that has already been (or will in the future be) delivered. "Rules and controls" may be delivered over a path different from the one **used** for **content** delivery. "rules and controls" may also be delivered at some other time. The content creator 102 might deliver content to content user 112 over the **electronic** highway 108, or could make the content available to anyone on the highway. **Content** may be **used** at the time it is delivered, or it may be stored for later use or reuse.

The virtual distribution environment 100 also allows payment and... ...to a certain limit) to pay for usage of any content. A "credit transaction" can take place at the user's site without requiring any "**online**" connection or further authorization. This invention can be used to help securely protect the virtual "credit card" against unauthorized use.

Rules and Contents" Define Processes... ...who lacks permission will not have her request satisfied ("No Go"). As another example, each user request to turn to a new page of an **electronic book** may be satisfied ("Go"), but it may not be necessary to meter, bill or budget those requests. A user who has purchased a copy of... ...can be charged to the user), and treat all later requests to open the same novel as "insignificant events." Other content (for example, searching an **electronic** telephone directory) may require the user to pay a fee for each access.

"Meter" process 404 keeps track of events, and may report usage to... ...content) into a "container" 302 so the information can't be accessed except as provided by its "rules and controls." Normally, the container 302 is **electronic** rather than physical. **Electronic** container 302 in one example comprises "**digital**" information having a well defined structure. Container 302 and its contents can be called an "object 300."

The Figure 5A example... ...a certain time. Even then, the container 302 "contains" the live feed (by reference) in this example.

Container 302 may contain information content 304 in **electronic** (such as "**digital**") form. Information content 304 could be the text of a novel, a picture, sound such as a **musical** performance or a reading, a **movie** or other video, computer software, or just about any other kind of **electronic** information you can think of. Other types of "object" 300 (such as "administrative objects") may contain "administrative" or other information instead of or in addition... ...IDREF=F0008>Figure 5B gives some additional detail about permissions record 808, budgets 308 and other methods 1000. The "permissions record"

808 specifies the **rights** associated with the object 300 such as, for example, who can open the container 302, who can use the object's contents, who can distribute the object, and what other control mechanisms must be active. For example, permissions record 808 may specify a user's **rights** to use, distribute and/or administer the container 302 and its content. Permissions record 808 may also specify requirements to be applied by the budgets... ...descrambled, and other processes associated with handling and controlling information content 304. For example, methods 1000 may record the identity of anyone who opens the **electronic** container 302, and can also control how information content is to be charged based on "metering." Methods 1000 may apply to one or several different... ...containers 302, as well as to all or specific portions of information content 304.

Secure Processing Unit (SPU)

The "VDE participants" may each have an "**electronic** appliance." The appliance may be or contain a computer. The appliances may communicate over the **electronic** highway 108. Figure 6 shows a secure processing unit ("SPU") 500 portion of the "**electronic** appliance" used in this example by each VDE participant. SPU 500 processes information in a secure processing environment 503, and stores important information securely. SPU 500 may be emulated by software operating in a host **electronic** appliance.

SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the... ...500 in this example is an integrated circuit ("IC") "chip" 504 including "hardware" 506 and "firmware" 508. SPU 500 connects to the rest of the **electronic** appliance through an "appliance link" 510. SPU "firmware" 508 in this example is "software" such as a "computer program(s)" "embedded" within chip 504. Firmware 508 makes the hardware 506 work. Hardware 506 preferably contains a processor to perform instructions specified by firmware 508. "Hardware" 506 also contains long-**term** and short-**term** memories to store information securely so it can't be tampered with. SPU 500 may also have a protected clock/calendar used for timing events. The SPU hardware 506 in this example may include special purpose **electronic** circuits that are specially designed to perform certain processes (such as "encryption" and "decryption") rapidly and efficiently.

The particular context in which SPU 500 is... ...in Figure 3. In some contexts, the functions of SPU 500 may be increased so the SPU can perform all the **electronic** appliance processing, and can be incorporated into a general purpose processor. In other contexts, SPU 500 may work alongside a general purpose processor, and therefore only needs to have enough processing capabilities to handle secure processes.

VDE **Electronic** Appliance and **Rights** Operating System"

Figure 7 shows an example of an **electronic** appliance 600 including SPU 500.
Electronic appliance 600 may be practically any kind of electrical or **electronic** device, such as:

C a computer

C a T.V. "set top" control box

C a pager

C a telephone

C a sound system

C a video reproduction system

C a video game player

C a "smart" credit card

Electronic appliance 600 in this example may include a keyboard or keypad 612, a voice recognizer 613, and a display 614. A human user can input... ...and may view information on display 614. Appliance 600 may communicate with the outside world through any of the connections/devices normally used within an **electronic** appliance. The connections/devices shown along the bottom of the drawing are examples:

a "modem" 618 or other telecommunications link;

a CD ROM disk 620... ...printer 622;

broadcast reception 624;

a document scanner 626; and

a "cable" 628 connecting the appliances with a "network."

Virtual distribution environment 100 provides a "**rights** operating system" 602 that manages appliance 600 and SPU 500 by controlling their hardware resources. The operating system 602 may also support at least one... ...602 provides a standardized, well defined, generalized "interface" that could support and work with many different "applications" 608.

Operating system 602 in this example provides "**rights** and auditing operating system functions" 604 and "other operating system functions" 606. The "**rights** and auditing operating system functions" 604 securely handle tasks that relate to virtual distribution environment 100. SPU 500 provides or supports many of the security functions of the

"**rights** and auditing operating system functions" 402. The "other operating system functions" 606 handle general appliance functions. Overall operating system 602 may be designed from the beginning to include the "**rights** and auditing operating system functions" 604 plus the "other operating system functions" 606, or the "**rights** and auditing operating system functions" may be an add-on to a preexisting operating system providing the "other operating system functions."

"**Rights** operating system" 602 in this example can work with many different types of appliances 600. For example, it can work with large mainframe computers, "minicomputers... ...also work in control boxes on the top of television sets, small portable "pagers," desktop radios, stereo sound systems, telephones, telephone switches, or any other **electronic** appliance. This ability to work on big appliances as well as little appliances is called "scalable." A "scalable" operating system 602 means that there can be a standardized interface across many different appliances performing a wide variety of tasks.

The "**rights** operating system functions" 604 are "services-based" in this example. For example, "**rights** operating system functions" 604 handle summary requests from application 608 rather than requiring the application to always make more detailed "subrequests" or otherwise get involved with the underlying complexities involved in satisfying a summary request. For example, application 608 may simply ask to read specified information; "**rights** operating system functions" 604 can then decide whether the desired information is VDE-protected content and, if it is, perform processes needed to make the information available. This feature is called "transparency." "Transparency" makes tasks easy for the application 608.

"**Rights** operating system functions" 604 can support applications 608 that "know" nothing about virtual distribution environment 100. Applications 608 that are "aware" of virtual distribution environment 100 may be able to make more detailed use of virtual distribution environment 100.

In this example, "**rights** operating system functions" 604 are "event driven". Rather than repeatedly examining the state of **electronic** appliance 600 to determine whether a condition has arisen, the "**rights** operating system functions" 604 may respond directly to "events" or "happenings" within appliance 600.

In this example, some of the services performed by "**rights** operating system functions" 604 may be extended based on additional "components" delivered to operating system 602. "**Rights** operating system functions" 604 can collect together and use "components" sent by different participants at different times. The "components" help to make the operating system... ...user). Other components are designed to work with specific applications or classes of applications (e.g., some types of meters and some types of budgets).

Electronic Appliance 600

An **electronic** appliance 600 provided by the preferred embodiment may, for example, be any **electronic** apparatus that contains one or more microprocessors and/or microcontrollers and/or other devices which perform logical and/or mathematical calculations. This may include computers; computer terminals; device controllers for use with computers; peripheral devices for use with computers; **digital** display devices; televisions; video and **audio**/video projection systems; channel selectors and/or decoders for use with broadcast and/or cable transmissions; remote control devices; video and/or **audio** recorders; media players including compact disc players, videodisc players and tape players; **audio** and/or video amplifiers; virtual reality machines; **electronic** game players; multimedia players; radios; telephones; videophones; facsimile machines; robots; numerically controlled machines including machine tools and the like; and other devices containing one or... ...microcomputers and/or microcontrollers and/or other CPUs, including those not yet in existence.

Figure 8 shows an example of an **electronic** appliance 600. This example of **electronic** appliance 600 includes a system bus 653. In this example, one or more conventional general purpose central processing units ("CPUs") 654 are connected to bus... ...for example, store information on mass media such as a tape 670, a floppy disk, a removable memory card, etc. Communications controller 666 may allow **electronic** appliance 600 to communicate with other **electronic** appliances via network 672 or other telecommunications links. Different **electronic** appliances 600 may interoperate even if they use different CPUs and different instances of ROS 602, so long as they typically use compatible communication protocols... ...comprise the same one or more non-secure secondary storage devices (such as a magnetic disk and a CD-ROM drive as one example) that **electronic** appliance 600 uses for general secondary storage functions. In some implementations, part or all of secondary storage 652 may comprise a secondary storage device(s... ...information.

Secondary storage 652 in this example stores code and data used by CPU 654 and/or SPU 500 to control the overall operation of **electronic** appliance 600. For example, Figure 8 shows that "**Rights** Operating System" ("ROS") 602 (including a portion 604 of ROS that provides VDE functions and a portion 606 that provides other OS functions) shown in... ...602 in particular may desirably be included in ROM 658 (e.g., "bootstrap" routines, POST routines, etc. for use in establishing an operating environment for **electronic** appliance 600 when power is applied).

Figure 8 shows that secondary storage 652 may also be used to store code ("application... ...not specifically designed for VDE 100) can also access and take advantage of VDE functions 604.

SECURE PROCESSING UNIT 500

Each VDE node or other **electronic** appliance 600 in the preferred embodiment may include one or more SPUs 500. SPUs 500 may be used to perform all secure processing for VDE... ...data management processes including governing usage of, auditing of, and where appropriate, payment for VDE objects 300 (through the use of prepayments, credits, real-time **electronic** debits from bank accounts and/or VDE node currency token deposit accounts). SPU 500 may perform other transactions related to such VDE objects 300. ...to complicate efforts to electrically determine the value of memory locations. These and other techniques may contribute to the security of barrier 502.

In some **electronic** appliances 600, SPU 500 may be integrated together with the device microcontroller or equivalent or with a device I/O or communications microcontroller into a... ...example, in one preferred embodiment, SPU 500 may be integrated together with one or more other CPU(s) (e.g., a CPU 654 of an **electronic** appliance) in a single component or package. The other CPU(s) 654 may be any centrally controlling logic arrangement, such as for example, a microprocessor... ...integrated SPU/CPU component is a standard feature of a widely distributed microprocessor line. Merging an SPU 500 into a main CPU 654 of an **electronic** appliance 600 (or into another appliance or appliance peripheral microcomputer or other microcontroller) may substantially reduce the overhead cost of implementing VDE 100. Integration considerations... ...may also be integrated into other peripheral devices, such as CD-ROM devices, set-top cable devices, game devices, and a wide variety of other **electronic** appliances that use, allow access to, perform transactions related to, or consume, distributed information.

SPU 500 Internal Architecture

Figure 9 is... ...be separate packages within a secure SPU 500.

In the preferred embodiment, microprocessor 520 normally handles the most security sensitive aspects of the operation of **electronic** appliance 600. For example, microprocessor 520 may manage VDE decrypting, encrypting, certain content and/or appliance usage control information, keeping track of usage of VDE secured content, and other VDE usage control related functions.

Stored in each SPU 500 and/or **electronic** appliance secondary memory 652 may be, for example, an instance of ROS 602 software, application programs 608, objects 300 containing VDE controlled property content and... ...VDE control information. ROS 602 includes software intended for execution by SPU microprocessor 520 for, in part, controlling usage of VDE related objects 300 by **electronic** appliance 600. As will be explained, these SPU programs include "load modules" for performing basic control functions. These various programs and associated data are executed... ...RTC 528, and may also maintain as non-volatile at least a portion of the otherwise volatile RAM 534 within SPU 500.

In one implementation, **electronic** appliance power supply 659 is also used to power SPU 500. Using any external power supply as the only power source for RTC 528 may... ...logic. In addition or alternatively, SPU 500 may from time to time compare an output of RTC 528 to a clock output of a host **electronic** appliance 600, if available. In the event a discrepancy is detected, SPU 500 may respond as appropriate, including recording the discrepancy and/or disabling at... ...and/or replacement data and/or code. In the event of a disabling and/or destruction of processes and/or information as described above, the **electronic** appliance 600 may require a secure VDE communication with an administrator, clearinghouse, and/or distributor as appropriate in order to reinitialize the RTC 528. Some... ...then.

It may be desirable to provide a mechanism for setting and/or synchronizing RTC 528. In the preferred embodiment, when communication occurs between VDE **electronic** appliance 600 and another VDE appliance, an output of RTC 528 may be compared to a controlled RTC 528 output time under control of the... ...objects handled by SPU 500. It is preferable that an extremely secure encryption/decryption technique be used as an aspect of authenticating the identity of **electronic** appliances 600 that are establishing a communication channel and securing any transferred permission, method, and administrative information. In the preferred embodiment, the encrypt/decrypt engine... ...The public/private key encryption/decryption circuit is used principally as an aspect of secure communications between an SPU 500 and VDE administrators, or other **electronic** appliances 600, that is between VDE secure subsystems. A symmetric encryption/decryption circuit may be used for "bulk" encrypting and decrypting most data stored in secondary storage 662 of **electronic** appliance 600 in which SPU 500 resides. The symmetric key encryption/decryption circuit may also be used for encrypting and decrypting content stored within VDE... ...otherwise be performed by software operating on microprocessor 520, or outside SPU 500. Decompression is important in the release of data such as video and **audio** that is usually compressed before distribution and whose decompression speed is important. In some cases, information that is useful for usage monitoring purposes (such as... ...unit 530 may be modelled after a USART or PCI bus interface in the preferred embodiment. In this example, BIU 530 connects SPU 500 to **electronic** appliance system bus 653 shown in Figure 8. BIU 530 is designed to prevent unauthorized access to internal components within SPU... ...memory:

1. (1) internal ROM 532;

2. (2) internal RAM 534; and

3. (3) external memory (typically RAM and/or disk supplied by a host **electronic** appliance).

The internal ROM 532 and RAM 534 within SPU 500 provide a secure operating environment and execution space. Because of cost limitations, chip fabrication... ...of sufficient speed and cost-effectiveness.

SPU External Memory

The SPU 500 can store certain information on memory devices external to the SPU. If available, **electronic** appliance 600 memory can also be used to support any device external portions of SPU 500 software. Certain advantages may be gained by allowing the... ...external memory. As one example, memory internal to SPU 500 may be reduced in size by using non-volatile read/write memory in the host **electronic** appliance 600 such as a non-volatile portion of RAM 656 and/or ROM 658.

Such external memory may be used to store SPU programs... ...stores in memory external to it.

SPU 500 can use a wide variety of different types of external memory. For example, external memory may comprise **electronic** appliance secondary storage 652 such as a disk; external EEPROM or flash memory 658; and/or external RAM 656. External RAM 656 may comprise an... ...not be necessary.

External memory used by SPU 500 may include two categories:

C external memory dedicated to SPU 500, and

C memory shared with **electronic** appliance 600.

For some VDE implementations, sharing memory (e.g., **electronic** appliance RAM 656, ROM 658 and/or secondary storage 652) with CPU 654 or other elements of an **electronic** appliance 600 may be the most cost effective way to store VDE secure database management files 610 and information that needs to be stored external... ...may be provided.

ROS Software Architecture

Figure 10 is a block diagram of one example of a software structure/architecture for **Rights** Operating System ("ROS") 602 provided by the preferred embodiment. In this example, ROS 602 includes an operating system ("OS") "core" 679, a user Application Program... ...503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources. A given **electronic** appliance 600 may include any number of SPE(s) 503 and/or any number of HPE(s) 655. HPE(s) 655 and SPE(s) 503...secure.

In the preferred embodiment, HPE 655 is a secure processing environment supported by a processor other than an SPU, such as for example an **electronic** appliance CPU 654 general-purpose microprocessor or other processing system or device. In the preferred embodiment, HYPE 655 may be considered to "emulate" an SPU... ...be provided in two types: secure and not secure. For example, it may be desirable to provide non-secure

versions of HPE 655 to allow **electronic** appliance 600 to efficiently run non-sensitive VDE tasks using the full resources of a fast general purpose processor or computer. Such non-secure versions... ...provide additional secure (albeit possibly less secure than the SPE) processing using host processor or other general purpose resources that may be available within an **electronic** appliance 600. Any service may be provided by such a secure HPE 655. In the preferred embodiment, certain aspects of "channel processing" appears to be... ...storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other **electronic** appliances 600; using kernel code that contains false branches and other complications in flow of control to disguise internal processes to some degree from disassembly... ...used for data values based on operational parameters to complicate efforts to manipulate such values; using any software and/or hardware memory management resources of **electronic** appliance 600 to "protect" the operation of HPE 655 from other processed, functions, etc. Although such a software-based tamper resistant barrier 674 may provide... ...by one or more secure HPEs 655 executing on general-purpose CPUs 654. Some VDE processes may not be allowed to proceed on reduced-security **electronic** appliances of this type if insufficient security is provided for the particular process involved.

Only those processes that execute completely within SPEs 503 (and in... ...679. They may also communicate messages directly with one another without messages going through OS "core" 679.

Kernel 680 may manage the hardware of an **electronic** appliance 600. For example, it may provide appropriate drivers and hardware managers for interacting with input/output and/or peripheral devices such as keyboard 612... ...manager 732 may route these RPCs to kernel 680 or elsewhere (e.g., to HPE(s) 655 and/or SPE(s) 503, or to remote **electronic** appliances 600, processors, or VDE participants) for processing. The API 682 may also service RPC requests by passing them to applications 608 that register to... ...628 for example), and routes one or more such data feeds appropriately while providing "translation" functions for real time data sent and/or received by **electronic** appliance 600 to allow "transparency" for this type of information analogous to the transparency provided by redirector 684 (and/or it may generate one or... ...modified control information set constitutes independent, secure delivery). For example, a content creator can produce a ROS 602 application that defines the circumstances required for **licensing** content contained within a VDE object 300. This application may reference structures provided by other parties. Such references might, for example, take the form of... ...by delivering different data elements defining pricing to different users. This attribute of supporting multiple party securely, independently deliverable control information is fundamental to enabling **electronic** commerce, that is, defining of a content and/or appliance control information set that represents the requirements of a collection of independent parties such as... ...N-level subassembly 690(k + N). The ability of ROS 602 to build component assemblies 690 out of other component assemblies provides great advantages in **terms** of, for example, code/data reusability, and the ability to allow different parties to manage different parts of an overall component.

Each component assembly 690... ...then the person could establish a price of zero instead of the price the content distributor intended to charge. Similarly, if the element establishes an **electronic** credit card, then an ability to substitute a different element could have disastrous consequences in **terms** of allowing a person to charge her usage to someone else's (or a non-existent) credit card. These are merely a few simple examples... ...data, requirements, and/or relationships for use in performing, and/or preparing to perform, basic instructions in relation to the operation of one or more **electronic** appliances 600. Basic instructions may be comprised of, for example:

C machine code of the type commonly used in the programming of computers; pseudo-code... ...use by an interpreter or other instruction processing program operating on a computer;

C a sequence of electronically represented logical operations for use with an **electronic** appliance 600;

C or other **electronic** representation of instructions, source code, object code, and/or pseudo code as those **terms** are commonly understood in the arts.

Information relating to said basic instructions may comprise, for example, data associated intrinsically with basic instructions such as for... ...1100 that perform the same or similar functions on different platforms, thereby making the method scalable and/or portable across a wide range of different **electronic** appliances.

UDEs 1200 and MDEs 1202 may store data for input to or output from executable component assembly 690 (or data describing such inputs and... ...a result, initial product implementation investment and complexity may be limited. The process of "surfacing" the full range of capabilities provided by ROS 602 in **terms** of authoring, administrative, and artificial intelligence applications may take place over time. Moreover, already-designed functionality of ROS 602 may be changed or enhanced at any time to adapt to changing needs or requirements.

More Detailed Discussion of **Rights** Operating System 602 Architecture

Figure 12 shows an example of a detailed architecture of ROS 602 shown in **electronic** appliance 600.

As mentioned above, three basic components of ROS 602 are a kernel 680, a Remote Procedure Call (RPC) manager 732 and an object... ...and the way they interact with other portions of ROS 602, will be discussed below.

Kernel 680

Kernel 680 manages the basic hardware resources of **electronic** appliance 600, and controls the basic tasking provided by ROS 602. Kernel 680 in the preferred embodiment may include a memory manager 680a, a task... ...manager 680a may manage allocation, deallocation, sharing and/or use of memory (e.g., RAM 656 shown in Figure 8) of **electronic** appliance 600, and may for example provide virtual memory capabilities as required by an **electronic** appliance and/or associated application(s). I/O manager 680c may manage all input to and output from ROS 602, and may interact with drivers... ...protocol may be used to conserve resources. This may limit the configurability of ROS 602 services, but this possible limitation may be acceptable in some **electronic** appliances.

The RPC structure allows services to be called/requested without the calling process having to know or specify where the service is physically provided... ...Procedure Calls" (RPCs) from a service requestor, and routes the service requests to a service provider(s) that can service the request. For example, when **rights** operating system 602 receives a request from a user application via user API 682, RPC manager 732 may route the service request to an appropriate... ...outgoing administrative objects;

Incoming Administrative Objects Manager 756 services requests relating to incoming administrative objects; and

Communications Manager 776 services requests relating to communications between **electronic** appliance 600 and the outside world.

Object Switch 734

Object switch 734 handles, controls and communicates (both locally and remotely) VDE objects 300. In the... ...780 and a mail gateway (manager) 782. Mail gateway 782 may include one or more mail filters 784 to, for example, automatically route VDE related **electronic** mail between object switch 734 and the outside world **electronic** mail services. External Services Manager 772 may interface to communications manager 776 through a Service Transport Layer 786. Service Transport Layer 786a may enable External... ...754

Outgoing administrative object manager 754 receives administrative objects from object switch 734, object repository manager 770 or other source for transmission to another VDE **electronic** appliance. Outgoing administrative object manager 754 takes care of sending the outgoing object to its proper destination. Outgoing administrative object manager 754 may obtain routing... ...transmitted, and other information related to transmission of objects.

Incoming Administrative Object Manager 756

Incoming administrative object manager 756 receives administrative objects from other VDE **electronic** appliances 600 via communications manager 776. It may route the object to object repository manager 770, object switch 734 or other destination. Incoming administrative object... ...objects 300 (administrative objects).

Figure 12A shows how object submittal manager 774 may be used to communicate with a user of **electronic** appliance 600 to help to create a new VDE object 300. Figure 12A shows that object creation may occur in two... ...503 to create secure data control structures). Container manager 764 may then write the new object to object repository 687, and the user or the **electronic** appliance may "register" the new object by including appropriate information within secure database 610.

Communications Subsystem 776

Communications subsystem 776, as discussed above, may be... ...from a cable, satellite or other telecommunications link.

Secure Processing Environment 503

As discussed above in connection with Figure 12, each **electronic** appliance 600 in the preferred embodiment includes one or more SPEs 503 and/or one or more HPEs 655. These secure processing environments each provide... ...ROS 602, and they may themselves generate service requests to be satisfied by other services within ROS 602 or by services provided by another VDE **electronic** appliance 600 or computer.

In the preferred embodiment, an SPE 503 is supported by the hardware resources of an SPU 500. An HPE 655 may... ...602 (although ROS 602 may be restricted from sending to an HPE certain highly secure tasks to be executed only within an SPU 500).

Some **electronic** appliance 600 configurations might include both an SPE 503 and an HPE 655. For example, the HPE 655 could perform tasks that need lesser (or...field 597(1), a user ID field 597(2), an object ID field 597(3), a field containing a reference or other identification to a "**right**" (i.e., a collection of events supported by methods referenced in a PERC 808 and/or "user **rights** table" 464) 597(4), an event queue 597(5), and one or more fields 598 that cross-reference particular event codes with channel detail records... ...preferred embodiment. In the preferred embodiment, a channel 594 provides event processing for a particular VDE object 300, a particular authorized user, and a particular "**right**" (i.e., type of event). These three parameters may be passed to SPE 503. Part of SPE kernel/dispatcher 552 executing within a "channel 0... ...1127). In the preferred embodiment, this "blueprint" may comprise a PERC 808 and/or URT 464. In may be obtained by using the "Object, User, **Right**" parameters passed to the "open channel" routine to "chain" together object registration table 460 records, user/object

table 462 records, URT 464 records, and PERC... ...may write appropriate information to channel header 596 (block 1129). Such information may include, for example, User ID, Object ID, and a reference to the "**right**" that the channel will process. The preferred embodiment process may next use the "blueprint" to access (e.g, the secure database manager 566 and/or... ...needed to respond to the event. The number of channel detail records will depend on the number of events that can be serviced by the "**right**," as specified by the "blueprint" (i.e., URT 464). During this process, the control method will construct "swap blocks" to, in effect, set up all...the NVRAM 534b of SPU 500). These tags may be generated by key and tag manager 558. They are used to, for example, check access **rights** to, validate and correlate data elements. For example, they may be used to ensure components of the secured data structures are not tampered with outside... ...The event summaries may be maintained, analyzed and used by SPE 503 (HPE 655) or a VDE administrator to determine and potentially limit abuse of **electronic** appliance 600. In the preferred embodiment, such parameters may be stored in secure memory (e.g., within the NVRAM 534b of SPU 500).

There are... ...VDE administrators and/or distributors for overall budget. A VDE administrator may register for event summaries and an overall budget summary at the time an **electronic** appliance 600 is initialized. The overall budget summary may be reported to and used by a VDE administrator in determining distribution of consumed budget (for... ...mode may be used by VDE administrators to determine device usage. The limit mode may be used to limit tampering and attempts to misuse the **electronic** appliance 600. Exceeding a limit will result in SPE 503 (HPE 655) refusing to service user requests until it is reset by a VDE administrator... ...embodiment event summary data structure:

Another, "overall currency budget" summary data structure maintained by the preferred embodiment summary services manager 560 allows registration of VDE **electronic** appliance 600. The first entry is used for an overall currency budget consumed value, and is registered by the VDE administrator that first initializes SPE... ...public key (or others) challenge-response protocol. This protocol is discussed in further detail elsewhere in this document. Tickets identify users with respect to the **electronic** appliance 600 in the case where the appliance may be used by multiple users. Tickets may be requested by and returned to VDE software applications... ...IDs and transaction tags for items that have identical distributor ID, item ID, and user ID fields (site ID will be fixed for a given **electronic** appliance 600). These four pieces of information may thus be used as hash algorithm parameters.

The "hash" pages may themselves be frequently updated, and should... ...written out.

As an alternative to the hash-based approach, if the number of updatable items is kept small (such as in a dedicated consumer **electronic** appliance 600), then assigning each updatable item a unique sequential site record number as part of its VDE item ID may allow a look up... ...engine 522.

VDE Secure Database 610

VDE 100 stores separately deliverable VDE elements in a secure (e.g., encrypted) database 610 distributed to each VDE "**electronic** appliance 610. The database 610 in the preferred embodiment may store and/or manage three basic classes of VDE items:

VDE objects,

VDE process elements... ...data structures.

The following table lists examples of some of the VDE items stored in or managed by information stored in secure database 610:

Each **electronic** appliance 600 may have an instance of a secure database 610 that securely maintains the VDE items. Figure 16 shows one... ...provided by the preferred embodiment.

The generalized "logical object" structure 800 shown in Figure 17 used by the preferred embodiment supports **digital** content delivery over any currently used media. "Logical object" in the preferred embodiment may refer collectively to: content; computer software and/or methods used to... ...software and/or methods. Logical objects may or may not be stored, and may or may not be present in, or accessible to, any given **electronic** appliance 600. The content portion of a logical object may be organized as information contained in, not contained in, or partially contained in one or... ...or to perform an administrative-type activity. Container 302 typically includes identifying information, control structures and content (e.g., a property or administrative data). The **term** "container" is often (e.g., Bento/OpenDoc and OLE) used to describe a collection of information stored on a computer system's secondary storage system... ...or be owned by the same entity. Rather, in VDE 100 the container concept is extended and generalized to include real-time content and/or **online** interactive content passed to an **electronic** appliance over a cable, by broadcast, or communicated by other **electronic** communication means.

Thus, the "complete" VDE container 302 or logical object structure 800 may not exist at the user's location (or any other location... ...provided by the preferred embodiment includes a public (or unencrypted) header 802 that identifies the object and may also identify one or more owners of **rights** in the object and/or one or more distributors of the object. Private (or encrypted) header 804 may include a part or all of the... ...attempts to register as a user of the object with a service clearinghouse, VDE administrator, or an SPU 500. Alternatively, information identifying one or more **rights** owners and/or distributors of the object may be located in encrypted form within encrypted header 804, along with any of said additional validating and... ...object 300.

The content portion of the object is typically divided into portions called data blocks 812. Data blocks 812 may contain any sort of **electronic** information, such as, "content," including computer programs, images, sound, VDE administrative information, etc. The

size and number of data blocks 812 may be selected by... ...of the sender and receiver. As a result, permission records 808 and key blocks 810 will frequently, in the preferred embodiment, be stored only on **electronic** appliances 600 of registered users (and may themselves be delivered to the user as part of a registration/initialization process). In this instance, permission records...example of a "Stationary Object" structure 850 provided by the preferred embodiment. "Stationary Object" structure 850 is intended to be used only at specific VDE **electronic** appliance/installations that have received explicit permissions to use one or more portions of the stationary object. Therefore, stationary object structure 850 does not contain... ...808 within private header 804. The inclusion of PERC 808 within traveling object structure 860 permits the traveling object to be used at any VDE **electronic** appliance/participant 600 (in accordance with the methods 1000 and the contained PERC 808).

"Traveling" objects are a class of VDE objects 300 that can specifically support "out of channel" distribution. Therefore, they include key block(s) 810 and are transportable from one **electronic** appliance 600 to another. Traveling objects may come with a quite limited usage related budget so that a user may use, in whole or part, content (such as a computer program, game, or database) and evaluate whether to acquire a **license** or further **license** or purchase object content. Alternatively, traveling object PERCs 808 may contain or reference budget records with, for example:

1. (a) budget(s) reflecting previously purchased **rights** or credit for future **licensing** or purchasing and enabling at least one or more types of object content usage, and/or

2. (b) budget(s) that employ (and may debit... ...the traveling object after the exhaustion of an available budget(s) or if the traveling object (or a copy thereof) is moved to a different **electronic** appliance and the new appliance does not have a available credit budget(s) that corresponds to the requirements stipulated by permissions record 808.

For example... ...budget that may be object independent and may be applied towards the use of a certain or classes of traveling object content (for example any **movie** object from a class of traveling objects that might be Blockbuster Video rentals). The budget VDE itself may stipulate one or more classes of objects... ...a manner as to allow correct referencing and to enable billing handling and resulting payments.

Traveling objects can be used at a receiving VDE node **electronic** appliance 600 so long as either the appliance carries the correct budget or budget type (e.g. sufficient credit available from a clearinghouse such as... ...object, if the user (and/or installation) doesn't have the appropriate budget(s) and/or authorizations, then the user could be informed by the **electronic** appliance 600 (using information stored in the traveling object) as to which one or more parties the user could contact. The party or parties might... ...require widely available budgets and may particularly benefit from out-of-channel distribution (e.g., credit card derived budgets for objects containing properties such as **movies**, software programs, games, etc.). Such traveling objects may be supplied with or without contained budget UDEs.

One use of traveling objects is the publishing of... ...to use the software in a demonstration mode, and possibly to use the full program features for a limited time before having to pay a **license** fee, or before having to pay more than an initial trial fee. For example, using a time based billing method and budget records with a... ...correspond to the time the user came into possession of the object.

Traveling objects can also be used to facilitate "moving" an object from one **electronic** appliance 600 to another. A user could move a traveling object, with its incorporated one or more permission records 808 from a desktop computer, for... ...or other security functions. Contained administrative object(s) may be used to install necessary permission records and/or budget information in the end user's **electronic** appliance.

Content Objects

Figure 20 shows an example of a VDE content object structure 880. Generally, content objects 880 include or provide information content. This "content" may be any sort of **electronic** information. For example, content may include: computer software, **movies**, **books**, **music**, information databases, multimedia information, virtual reality information, machine instructions, computer data files, communications messages and/or signals, and other information, at least a portion of which is used and/or manipulated by one or more **electronic** appliances. VDE 100 can also be configured for authenticating, controlling, and/or auditing **electronic** commercial transactions and communications such as inter-bank transactions, **electronic** purchasing communications, and the transmission of, auditing of, and secure commercial archiving of, electronically signed contracts and other legal documents; the information used for these... ...single object to contain one or more content containing objects and one or more administrative objects. Administrative objects may be used to transmit information between **electronic** appliances for update, usage reporting, billing and/or control purposes. They contain information that helps to administer VDE 100 and keep it operating properly. Administrative objects generally are sent between two VDE nodes, for example, a VDE clearinghouse service, distributor, or client administrator and an end user's **electronic** appliance 600.

Administrative object structure 870 in this example includes a public header 802, private header 804 (including a "PERC" 808) and a "private body... ...purchase, a purchase order, or an invoice. Each event record 872 may be a set of instructions to be executed by the end user's **electronic** appliance 600 to make an addition or modification to the end user's secure database 610, for example. Events can perform many basic management functions, for example: add an object to the object registry, including providing the associated user/group record(s), **rights** records, permission record and/or method records; delete audit records (by "rolling up" the audit trail information into, for example, a more condensed, e.g. summary form, or by actual deletion); add or update permissions records 808 for previously registered objects; add or update budget records; add or update user **rights** records; and add or update load modules.

In the preferred embodiment, an administrative object may be sent, for example, by a distributor, client administrators, or... ...requirements and/or relationships for use in performing, and/or preparing to perform, the basic instructions in relation to the operation of one or more **electronic** appliances 600. As shown in Figure 16, methods 1000 in the preferred embodiment are represented in secure database 610 by:

C... ...reference one or more DTD and/or MDE data structures that contain a textual description of their operations suitable for inclusion as part of an **electronic** contract. The references to the DTD and MDE data structures may occur in the private header of the method core 1000', or may be specified...a method core 1000N references a load module 1100, a load module is loaded into the SPE 503, decrypted, and then either passed to the **electronic** appliance microprocessor for executing in an HPE 655 (if that is where it executes), or kept in the SPE (if that is where it executes... ...on which it operates. Initiation of load module execution in this environment is strictly controlled by a combination of access tags, validation tags, encryption keys, **digital** signatures and/or correlation tags. Thus, a load module 1100 may only be referenced if the caller knows its ID and asserts the shared secret... ...values that can be placed in the fields. Other DTDs may describe the function of the load module 1100 in English for inclusion in an **electronic** contract, for example.

The next section of load module 1100 is an encrypted executable body 1106 that contains one or more blocks of encrypted code...

Claims: ...B1

1. Procede de traitement d'un contenu **digital** electronique en utilisant un environnement d'exploitation securitaire (602) au niveau de l'appareil electronique d'un utilisateur (600), ledit procede comprenant les etapes de :reception d'un objet a contenu (880) contenant ledit contenu **digital** audit environnement d'exploitation securitaire (602);

       stockage de l'objet a contenu audit environnement d'exploitation securitaire;

       recevoir separement et de facon securitaire un premier... ...d'exploitation securitaire, ledit premier objet administratif comprenant des donnees specifiant une premiere regle liee a l'utilisation identifiant une premiere utilisation permise du contenu **digital** electronique;

stockage desdites donnees specifiant une premiere regle liee a l'utilisation audit environnement d'exploitation securitaire;

recevoir separement et de facon securitaire un deuxieme... ...d'exploitation securitaire, ledit deuxieme objet administratif comprenant des donnees specifiant une deuxieme regle liee a l'utilisation identifiant une deuxieme utilisation permise du contenu **digital** electronique;

stockage desdites donnees specifiant une deuxieme regle liee a l'utilisation audit environnement d'exploitation securitaire;

de traiter de facon securitaire l'objet a... ...dans le premier objet administratif et la deuxieme regle liee a l'utilisation contenue dans le deuxieme objet administratif pour regir l'utilisation dudit contens **digital** electronique au niveau de l'appareil electronique de l'utilisateur,

dans lequel l'une de la premiere regle liee a l'utilisation et de la deuxieme regle liee a l'utilisation commande l'etape de traitement en specifiant un emplacement pour l'insertion d'une empreinte au niveau du contenu **digital** electronique de sorte que, lorsque le contenu est libere en clair, les informations representant une identification de l'utilisateur et/ou l'appareil electronique de... ...contenant de logiciel.

14. Procede selon l'une quelconque des revendications precedentes, dans lequel ladite etape de traitement securitaire comprend l'utilisation mesuree dudit contenu **digital** electronique et/ou desdites regles liees a l'utilisation.

15. Procede selon l'une quelconque des revendications precedentes, dans lequel l'etape de traitement securitaire comprend la verification de l'utilisation dudit contenu **digital** electronique et/ou desdites regles liees a l'utilisation.

16. Procede selon l'une quelconque des revendications precedentes, dans lequel ladite etape de traitement securitaire comprend la prevision du budget de l'utilisation du contenu **digital** electronique et/ou desdites regles liees a l'utilisation.

17. Procede selon l'une quelconque des revendications precedentes, dans lequel au moins un dudit premier... ...relation securitaire entre au moins une de ladite premiere regle liee a l'utilisation et ladite deuxieme regle liee a l'utilisation, et ledit contenu **digital** electronique.

21. Procede selon l'une quelconque des revendications precedentes, dans lequel ladite etape de traitement securitaire comprend l'etape consistant a acceder a une... ...ladite deuxieme entite etant distincte de la premiere entite.

31. Appareil electronique utilisateur pour le traitement d'un objet a contenu (880) contenant un contenu **digital** electronique, l'appareil comprenant :un environnement d'exploitation securitaire (602);

des moyens (776) pour recevoir l'objet a contenu (880) audit environnement d'exploitation securitaire... ...securitaire, ledit premier objet administratif comprenant la specification des donnees d'une premiere regle liee a l'utilisation identifiant une premiere utilisation permise du contenu **digital** electronique (880);

des moyens (776) pour recevoir separement et de facon securitaire un deuxieme objet administratif (870) audit environnement d'exploitation securitaire (602) a partir... ...securitaire, ledit deuxieme objet administratif comprenant la specification des donnees d'une deuxieme regle liee a l'utilisation identifiant une deuxieme utilisation permise du contenu **digital** electronique; et

une base de donnees securitaire (610) pour le stockage des donnees specifiant une premiere regle liee a l'utilisation et des donnees specifiant...

...le premier objet administratif et la deuxieme regle liee a l'utilisation contenue dans le deuxieme objet administratif afin de regir l'utilisation dudit contenu **digital** electronique au niveau de l'appareil electronique de l'utilisateur; et

dans lequel ledit environnement de traitement securitaire (602) est agence tel que l'une... ...deuxieme regle liee a l'utilisation commande l'environnement de traitement securitaire en specifiant un emplacement pour l'insertion d'une empreinte dans le contenu **digital** electronique de sorte que, lorsque le contenu est libere en clair, les informations representant une identification de l'utilisateur et/ou de l'appareil electronique...

18/K/13 (Item 1 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

Country	Number	Kind	Date

Detailed Description:

...the digest algorithm used for the included parts (default is MD-5) Description of the algorithm used for the digital signature encryption (default is RSA) **Digital** signature (encrypted digest of all of the concatenated digests of the included parts) SC(s) may include more than one BOM. For example, an Offer SC(s) 641 consists of the original Metadata SC(s) 620 parts, including its BOM, as well as additional information added by the **Electronic Digital** Content Storc(s) 103 and a new BOM. A record for the Metadata SC(s) 620 BOM is included in the Offer SC(s) 641... ...the Metadata SC(s) 620 have records in the new BOM that was created for the Offer SC(s) 641. Only parts added by the **Electronic Digital** Content Store(s) 103 and the Metadata, SC(s) 620 BOM have records in the new BOM.

SC(s) may also include a Key Description the encrypted part.

If the SC(s) does not contain any encrypted parts, then there is no Key Description part.

B. **Rights** Management Language Syntax and Semantics
The **Rights** Management Language consists of parameters that can be assigned values to define restrictions on the use of the Content I 1 3 by an End... ...the Content 113 is the Usage Conditions 517. Each Content Provider(s) 101 specifies the Usage Conditions 517 for each of its Content 113 items. **Electronic Digital** Content Store(s) 103 interpret the Usage Conditions 517 in Metadata SC(s) 620 and use the information to provide select options they wish to... ...the End-User Device(s) 109 requests authorization for the Content 113 based on Store Usage Conditions 519. Before the Clearinghouse(s) 105 sends a **License** SC(s) 660 to the End-User(s), the Clearinghouse(s) 105 verifies that the Store Usage Conditions 519 being requested are in agreement with... ...Content 1 1 3 are enforced.

The following are examples of Store Usage Conditions 519 for an embodiment where the Content 1 1 3 is **music**.

Song is recordable.

Song can be played n number of times.

C. Overview of Secure Container Flow and Processing
Metadata SC(s) 620 are built by Content Provider(s) I 0 1 and are **used** to define **Content** 1 1 3 items such as songs. The Content 113 itself is not included in these SC(s) because the size of the Content 113 is typically too large for **Electronic Digital** Content Store(s) 103 and End- User(s) to efficiently download the containers just for the purpose of accessing the descriptive metadata. Instead, the SC... ...113. The SC(s) also includes metadata that provides descriptive information about the Content 1 1 3 and any other associated data, such as for **music**, the CD cover art and/or **digital audio** clips in the case of song Content II 3.

Electronic Digital Content Store(s) 103 download the Metadata SC(s) 620, for which they are authorized, and build Offer SC(s) 641. In short, an Offer SC(s) 641 consists of some of the parts and the BOM from the Metadata SC(s) 620 along with additional information included by the **Electronic Digital** Content Store(s) 101 A new BOM for the Offer SC(s) 641 is created when the Offer SC(s) 641 is built. **Electronic Digital** Content Store(s) 103 also use the Metadata SC(s) 620 by extracting metadata information from them to build HTML pages on their **web** sites that present descriptions of Content I 1 3 to End-User(s), usually so they can purchase the Content 1 1 3.

The information in the Offer SC(s) 641 that is added by the **Electronic Digital** Content Store(s) 103 is typically to narrow the selection of Usage Conditions 517 that are specified in the Metadata SC(s) 620 and promotional data such as a graphic image file of the store's logo and a URL to the store's **web** site. An Offer SC(s) template in the Metadata SC(s) 620 indicates which information can be overridden by the **Electronic Digital** Content Store(s) 103 in the Offer SC(s) 641 and what, if any, additional information is required by the **Electronic Digital** Content Store(s) 103 and what parts are retained in the embedded Metadata SC(s) 620.

Offer SC(s) 641 are included in a Transaction SC(s) 640 when an End-User(s) decides to purchase Content 113 from an **Electronic Digital** Content Store(s) 103. The **Electronic Digital** Content Store(s) 103 builds a Transaction SC(s) 640 and includes Offer SC(s) 641 for each Content 113 item being purchased and transmits... ...Clearinghouse(s) 105 validates and processes Order SC(s) 650 to provide the End- User Device(s) 109 with everything that is required to a **License** Watermark 527 and access purchased Content 113. One of the functions of the Clearinghouse(s) 105 is to decrypt the Symmetric Keys 623 that are...the SC(s) and encrypts them again with the Public Key 661 of the End-User Device(s) 109. The Clearinghouse(s) 105 builds a **License** SC(s) 660 that includes the newly encrypted Symmetric Keys 623 and updated watermarking instructions and sends it to the End-User Device(s) 109... ...the Clearinghouse(s) 105 returns to the End-User Device(s) 109 an HTML page or equivalent reporting the failure of the authorization process.

A **License** SC(s) 660 provides an End-User Device(s) 109 with everything that is needed to access a Content 113 item. The End-User Device... ...IO 1 and include encrypted Content 1 1 3 and metadata parts. The End-User Player Application 195 uses the Symmetric Keys 623 from the **License** SC(s) 660 to decrypt the Content II 3, metadata, and watermarking instructions. The watermarking instructions are then affixed into the Content II 3 and... ...template), although the entire original BOM is propagated. This is done because the entire BOM is required by the Clearinghouse(s) 105 to verify the **digital** signature in the original SC(s).

The Key Description Part columns of the following table define the records that are included in the Key Description... ...Enc Syrn RSA CH Pub
Part Key Key
SC Version
SC ID
SC Type
SC Publisher
Date
Expiration Date
Clearinghouse(s)
URL
Digest Algorithm ID
Digital Signature Alg
ID
Content ID Yes Yes
Metadata Yes Yes
Usage Conditions Yes Yes
SC Templates Yes Yes
Watermarking Yes Yes Output RC4 Enc Sym... ...CH Pub
Instructions Part Key Key
Key Description Part Yes Yes
Clearinghouse(s) Yes No

Certificate(s) I I
Certificate(s) Yes I No
I **Digital** Signature
The following describes the **terms** that are used in the above Metadata SC(s) table.

[Content URL] - A parameter in a record in the Key Description part. This is a...use of the Content 113.

SC(s) Templates - Parts that define templates that describe the required and optional information for building the Offer, Order, and **License** SC(s) 660.

Watermarking Instructions - A part that contains the encrypted instructions and parameters for implementing watermarking in the Content 113. The watermarking instructions may be modified by the Clearinghouse(s) 105 and returned back to the End-User Device(s) 109 within the **License** SC(s) 660.

There is a record in the Key Description part that defines the encryption algorithm that was used to encrypt the watermarking instructions... ...proper authorization to access the Content 1 1 3.

Digest Algorithm ID - An identifier of the algorithm used to compute the digests of the parts.

Digital Signature Alg ID - An identifier of the algorithm used to encrypt the digest of the concatenated part digests. This encrypted value is the **digital** signature.

Digital Signature - A digest of the concatenated part digests encrypted with the public key of the entity that created the SC(s).

Output Part - The name... ...Sym RSA CH Pub
I Part Key Key
SC Version
SC ID
SC Type
SC Publisher
Date
Expiration Date
Clearinghouse(s)
URL
Digest Algorithm ID
Digital Signature Aig
ID
Content ID Yes Yes
Metadata Some Yes
Usage Conditions Yes Yes
SC Templates Yes Yes

Watermarking Yes Yes Output RC4 Enc: Sym... ...CH Pub
Instructions I I I Part Key Key
Key Description Part Yes Yes
Clearinghouse(s) Yes No
Certificate(s)
Certificate(s) Yes No
I **Digital** Signature
--- Offer SC Parts -------------------------------

SC Version
SC ID
SC Type
SC Publisher
Date
Expiration Date
Digest Algorithm ID
Digital Signature Alg
ID
Metadata SC BOM Yes Yes
Additional and Yes Yes
Overridden Fields
Electronic Digital Yes No
Content Store(s)
Certificate
j Certificate(s) Y No
Digital Signature
The following describes the **terms** that are used in the above Offer SC(s) 641 that were
not previously described for another SC(s).

Metadata SC(s) BOM - The BOM... ...s) 641 BOM includes the digest of the Metadata
SC(s) 620 BOM.

Additional and Overridden Fields - Usage conditions information that was overridden by
the **Electronic Digital** Content Store(s) 103. This information is validated by the
Clearinghouse(s) 105, by means of the received SC(s) templates, to make sure that
anything that the **Electronic Digital** Content Store(s) 103 overrides is within the scope of
its authorization.

Electronic Digital Content Store(s) Certificate - A certificate provided to the **Electronic
Digital** Content Store(s) 103 by the Clearinghouse(s) 105 and signed by the
Clearinghouse(s) 105 using its private key.

This certificate is used by the End-User Player Application 195 to verify that the
Electronic Digital Content Store(s) 103 is a valid distributor of Content 113. The End-
User Player Application 195 and Clearinghouse(s) 105 can verify that the **Electronic
Digital** Content Store(s) 103 is an authorized distributor by decrypting the certificate's

signature with the Clearinghouse's 105 Public Key 621. The End-User... ...Key Parts Part Exists Digest Name Alg Enc Key Alg ID

SC Version

SC ID

SC Type

SC Publisher

Date

Expiration Date

Digest Algorithm ID

Digital Signature Alg

ID

Transaction ID Yes Yes Output RSA CH Pub

I I I Part Key

End-User(s) ID Yes Yes Output RSA CH... ...Public Yes Yes

Key

Offer SC(s) Yes Yes

Selections of Content Yes Yes

Use

HTML to Display Yes Yes

Key Description Part Yes Yes

Electronic Digital Yes No

Content Store(s)

Certificate

I **Digital** Signature

The following describes the **terms** that are used in the above Transaction SC(s) 640 that were not previously described for another SC(s).

Transaction ID 535 - An ID assigned by the **Electronic Digital** Content Store(s) 103 to uniquely identify the transaction.

End-User(s) ID - An identification of the End-User(s) obtained by the **Electronic Digital** Content Store(s) 103 at the time the End-User(s) makes the buying selection and provides the credit card information.

End-User(s)' Public... ...by the Clearingbouse(s) 105 to I 0 re-encrypt the Symmetric Keys 623. The End-User(s)' Public Key 661 is transmitted to the **Electronic Digital** Content Store(s) 103 during the purchase transaction.

Offer SC(s) - Offer SC(s) 641 for the Content 113 items that were purchased.

Selections of... ...entry for each Offer SC(s) 641.

HTML to Display - One or more HTML pages that the End-User Player Application 195 displays in the **Internet** browser window upon receipt of the Transaction SC(s) 640 or during the interaction between the End-User Device(s) 109 and the Clearinghouse(s... ...SC(s) 640, the following steps may be performed to verify the integrity and authenticity

of the SC(s).

I Verify the integrity of the **Electronic Digital** Content Store(s) 103 certificate using the Public Key 621 of the Clearinghouse(s) 105. The Public Key 621 of the Clearinghouse(s) 105 was... ...s) 109 after it was received as part of the initialization of the End-User Player Application 195 during its installation process.

2. Verify the **Digital** Signature 643 of the SC(s) using the public key from the **Electronic Digital** Content Store(s) 103 certificate.

I 0 3. Verify the hashes of the SC(s) parts.

4. Verify the integrity and authenticity of each Offer... ...I Part Key Key
SC(s) Version
SC(s) ID
SC(s) Type
SC(s) Publisher
Date
Expiration Date
Clearinghouse(s)
URL
Digest Algorithm ID
Digital Signature Alg
ID
Content ID Yes Yes
Metadata Some Yes
Usage Conditions Yes Yes
SC(s) Templates Yes Yes
Watermarking Yes Yes Output RC4 Enc Sym RSA CH Pub
Instructions Part Key Key
Key Description Part Yes Yes
Clearinghouse(s) Yes No
Certificate(s)
Certificate(s) No
Digital Signature
--------------------------- ---------- ----------- Offer SC(s) Parts ------------------------------- ------------------------
SC(s) Version
SC(s) ID
SC(s) Type
SC(s) Publisher
Date
Expiration Date
Digest Algorithm ID
Digital Signature Alg
I

Metadata SC(s) BOM Yes Yes
Additional and Yes Yes
Overridden Fields
Electronic Digital Yes No
Content
Store(s) Certificate
Certificate(s) es No
Digital Signature 11 I I I I

--- Transaction SC(s) Parts --------------------------- ------------- ----------

SC(s) Version
SC(s ID
SC(s) Type
SC(s) Publisher
Date
Expiration Date
Digest Algorithm ID
Digital Signature Alg
ID
Transaction ID Yes Yes Output RSA CH Pub
I I I Part Key
End-User(s) ID Yes Yes Output RSA CH...s) One Yes
Offer
SC(s)
Selections of Content es Yes
Use
HTML to Display in Yes Yes
Browser Wdw
Key Description Part Yes Yes
Electronic Digital Yes No
Content
Store(s) Certificate
Digital Signature

---------------------------- ------------------------ Order SC(s) Parts ---------------------------- -----------------------

SC(s) Version
SC(s) ID
SC(s) Type
SC(s) Publisher
Date
Expiration Date
Digest Algorithm ID
Digital Signature Alg
ID
Offer SC(s) BOM Yes Yes
Transaction SC(s) BOM Yes Yes

Encrypted Credit Card Yes Yes Output RSA CH Pub
Info Part Key
Key Description Part Yes Yes
Digital Signature
The following describes the **terms** that are used in the above Order SC(s) 650 that were
not previously described for another SC(s).

Transaction SC(s) BOM - The BOM... ...from the End-User(s) that is used to charge the
purchase to a credit card or debit card. This information is required when the **Electronic
Digital** Content Store(s) 103 that created the Offer SC(s) 641 does not handle the
customer billing, in which case the Clearinghouse(s) 105 may handle the billing
I 0 H. **License** Secure Container 660 Format
The following table shows the parts that are included in the **License** SC(s) 660 as well as
its BOM. As shown in the Key Description part, the Symmetric Keys 623 that are
required for decrypting the... ...been re-encrypted by the Clearinghouse(s) 105 using the
End-User(s)@ Public Key 661. When the End-User Device(s) 109 receives the **License**
SC(s) 660 it decrypts the Symmetric Keys 623 and use them to access the encrypted parts
ftom the **License** SC(s) 660 and the Content SC(s) 630.

Key Description Part
BOM Result Encrypt Key IDI Sym Ke.v Synt Key
Parts Part Exists... ...Sym RSA EU Pub
Part Key Key
SC(s) Version
SC(s) ID
SC(s) Type
SC(s) Publisher
Date
Expiration Date
Digest Algorithm ID
Digital Signature Alg
ID
Content ID Yes Yes
Usage Conditions Yes Yes
Transaction Data Yes Yes
Watermarking Yes Yes Output RC4 Eric Sym RSA EU Pub
Instructions Part Key Key
Key Description Yes Yes
Certificate(s) Yes No
Digital Signature
The following describes the **terms** that are used in the above **License** SC(s) 660 that were
not previously described for another SC(s).

EU Pub Key - An identifier that indicates that the End-User(s)' Public... ...Part Exists
Digest
SC(s) Version

SC(s) ID
SC(s) Type
SC(s) Publisher
Date
Expiration Date
Clearinghouse(s) 105
URL
Digest Algorithm ID
Digital Signature Alg
ID
Content ID Yes Yes
Encrypted Content Yes Yes
Encrypted Yes Yes
Metadata
Metadata Yes Yes
Certificate(s) Yes No
Digital Signature
The following describes the **terms** used in the above Content SC(s) 630 that were not previously described for another SC(s).

Encrypted Content - Content 1 1 3 that was... ...There is no Key Description part included in the Content SC(s) 630 since the keys required to decrypt the encrypted parts are in the **License** SC(s) 660 that is built at the Clearinghouse(s) 105.

VI. SECURE CONTAINER PACKING AND UNPACKING
A, Overview
The SC(s) Packer is a... ...specified parts. The SC(s) Packer 151, 152, 153 variety of hardware platforms supporting Windows' program at the Content Provider(s) 101, Clearinghouse(s) 105, **Electronic Digital** Content Store(s) 103 and other sites requiring SC(s) Packing. A BOM and, if necessary, a Key Description part are created and included in... ...Description parts and to include parts in the SC(s). Encryption of parts and Symmetric Keys 623 as well as computing the digests and the **digital** signature is also be performed by the packer. Encryption and digest algorithms that are supported by the packer are included in the packer code or...processed. Bundling the parts into a single object is the last step that is performed when building a SC(s).

Indication as to whether the **digital** signature is ornitted from the BOM part. If this flag is not set, then the **digital** signature is computed **right** before the SC(s) is bundled into a single object.

In an alternate embodiment, the interface to the packer for building a SC(s) is... ...on a single line with a new line indicating the start of a new record. The BOM usually includes digests for each part and a **digital** signature that can be used to validate the authenticity and integrity of the SC(s).

The record types within a BOM are as follows.

IP... ...the type of the SC(s), which should be one ofORD - An Order SC(s) 650.

OFF - An Offer SC(s) 64 1.

LIC - A **License** SC(s).

TRA - A Transaction SC(s) 640.

MET - A Metadata SC(s) 620.

CON - A Content SC(s) 630.

A value
The A property...Specifies the Key Description part.

W part-name [digest]
Specifies the watermarking instructions part.

C parLname [digest]
Specifies the certificate(s) used to validate the **digital** signature.

T part-name [digest]
Specifies the Usage Conditions part.

I 0
YF part-name [digest]
Specifies the Template part for the Offer SC(s... ...1.

YO part-name [digest]
Specifies the Template part for the Order SC(s) 650.

YL part-name [digest]
Specifies the Template part for the **License** SC(s) 660.

ID part-name [digest]
Specifies the ID(s) of the Content 1 1 3 of the itern(s) of Content 1 13 being referenced.

CH part-name [digest]
Specifies the Clearinghouse(s) 105 certificate part.

SP part-name [digest]
Specifies the **Electronic Digital** Content Store(s) 103 certificate part.

B part-name [digest]
Specifies a BOM part for another SC(s) that has its parts or a subset... ...parameter.

D part-name [digest]
Specifies a data (or metadata) part.

S An S record is a signature record -the is used to define the **digital** signature of the
SC(s). The **digital** signature is specified as follows.

S key-identifier signatureLstring signature-algorithm
The S record contains the keyidentifier to indicate the encryption key of the signature, the
I 0 signature-string, which is the base64 encoding of the **digital** signature bitstring, and
the signature algorithm that was used to encrypt the digest to create the **digital** signature.

C. Key Description Part
The Key Description part is created by the packer to provide information about
encryption keys that are needed for decryption... ...Key 623 bit string that was used to
encrypt the part.

VIL CLEARINGHOUSE(S) 105
A. Overview
The Clearinghouse(s) 105 is responsible for the **rights** management functions of the
Secure **Digital** Content **Electronic** Distribution System 100. Clearinghouse(s) 105
functions include enablement of **Electronic Digital** Content Store(s) 103, verification of
rights to Content 113, integrity and authenticity validation of the buying transaction and
related information,.distribution of Content encryption keys or Symmetric Keys 623 to
End-User Device(s) 109, tracking the distribution of those keys, and reporting of
transaction summaries to **Electronic Digital** Content Store(s) 103 and Content
Provider(s) 101. Content encryption keys are used by End-User Device(s) 109 to unlock
Content 113 for which they have obtained **rights**, typically by a purchase transaction
from an authorized **Electronic Digital** Content Store(s) 103. Before a Content encryption
key is sent to an End-User Device(s) 109, the Clearinghouse(s) 105 goes through a
verification process to validate the authenticity of the entity that is selling the Content 1 1
3 and the **rights** that the End-User Device(s) 109 has to the Content 113. This is called
the SC Analysis Tool 185. In some configurations the Clearinghouse... ...may also handle
the financial settlement of Content I 1 3 purchases by co-locating a system at the
Clearinghouse(s) 105 that performs the **Electronic Digital** Content Store(s) 103 functions
of credit card authorization and billing. The Clearinghouse(s) 105 uses OEM packages
such as ICVerify and Taxware to handle the credit card processing and local sales taxes.

Electronic Digital Content Store(s) Embodiment
An **Electronic Digital** Content Store(s) 103 that wants to participate as a seller of
Content 113 in the Secure **Digital** Content **Electronic** Distribution System 100 makes a
request to one or more of the **Digital** Content Provider(s) I 01 that provide Content 1 1 3
to the Secure **Digital** Content **Electronic** Distribution System 1 00. There is no definitive
process for making the request so long as the two parties come to an agreement. After the
digital content label such as a **Music** Label e.g. Sony, Time-Warner, etc. decides to allow
the **Electronic Digital** Content Store(s) 103 to sell its Content 113, the Clearinghouse(s)

105 is contacted, usually via E-mail, with a request that the **Electronic Digital** Content Store(s) 103 be added to the Secure **Digital** Content **Electronic** Distribution System 100. The **digital** content label provides the name of the **Electronic Digital** Content Store(s) 103 and any other information that may be required for the Clearinghouse(s) 105 to create a **digital** certificate for the **Electronic Digital** Content Store(s) 103. The **digital** certificate is sent to the **digital** content label in a secure fashion, and then forwarded by the **digital** content label to the **Electronic Digital** Content Store(s) 103. The Clearinghouse(s) 105 maintains a database of **digital** certificates that it has assigned. Each certificate includes a version number, a unique serial number, the signing algorithm, the name of the issuer (e.g., the name of Clearinghouse(s) 105), a range of dates for which the certificate is considered to be valid, the name **Electronic Digital** Content Store(s) 103, the public key of the **Electronic Digital** Content Store(s) 103, and a hash code of all of the other information signed using the private key of the Clearinghouse(s) 105. Entities... ...that a SC(s) with a signature that can be validated using the public key from the certificate is a valid SC(s).

After the **Electronic Digital** Content Store(s) 103 has received its **digital** certificate that was created by the Clearinghouse(s) 105 and the necessary tools for processing the SC(s) from the **digital** content label, it can begin offering Content 113 that can be purchased by End-User(s). The **Electronic Digital** Content Store(s) 103 includes its certificate and the Transaction SC(s) 640 and signs the SC(s) using its **Digital** Signature 643. The End-User Device(s) 109 verifies that the **Electronic Digital** Content Store(s) 103 is a valid distributor of Content 113 on the Secure **Digital** Content **Electronic** Distribution System 100 by first checking the **digital** certificate revocation list and then using the Public Key 621 of the Clearinghouse(s) 105 to verify the information in the **digital** certificate for the **Electronic Digital** Content Store(s) 103. A **digital** certificate revocation list is maintained by the Clearinghouse(s) 105. The revocatim list may be included as me of the parts in a **License** SC(s) 660 that is I 0 created by the Clearinghouse(s) 105. End-User Device(s) 109 keep a copy of the revocation list on the End-Uscr Device(s) 109 so they can use it as part of the **Electronic Digital** Content Store(s) 103 **digital** certificate validation.

Whenever the End-User Device(s) 109 receives a **License** SC(s) 660 it determines whether a new revocation list is included and if so, the local revocation list on the End-User Device(s) 109 is updated.

B. **Rights** Management Processing
Order SC(s) Analysis
The Clearinghouse(s) 105 receives an Order SC(s) 650 from an End-User(s) after the End-User(s) has received the Transactim SC(s) 640, which include the Offer SC(s) 641, from the **Electronic Digital** Content Store(s) 103. The Order SC(s) 650 consists of parts that contain information relative to the Content 113 and its use, informatim about the **Electronic Digital** Content Store(s) 103 that is selling the Content 1 1 3, and information about the End-User(s) that is purchasing the Content 113... ...it contains has not been corrupted in any way.

Validation

The Clearinghouse(s) 105 begins the validation of Order SC(s) 650 by verifying the **digital** signatures, then the Clearinghouse(s) 105 verifies the integrity of the Order SC(s) 650 parts. To validate the **digital** signatures, first the Clearinghouse(s) 105 decrypts the Contents 631 of the signature itself using the Public Key 661 of the signing entity included if signed. (The signing entity could be the Content Provider(s) 101, the **Electronic Digital** Content Store(s) 103, the End User Device(s) 109 or any combination of them.) T en, the Clearinghouse(s) 105 calculates the digest of the concatenated part digests of the SC(s) and compares it with the **digital** signature's decrypted Content 113. if the two values match, the **digital** signature is valid. To verify the integrity of each part, the Clearinghouse(s) 105 computes the digest of the part and compares it to the digest value in the BOM. The Clearinghouse(s) 105 follows the same process to verify the **digital** signatures and part integrity for the Metadata and Offer SC(s) 641 parts included within the Order SC(s) 650.

The process of verification of the Transaction and Offer SC(s) 641 **digital** signatures also indirectly verifies that the **Electronic Digital** Content Store(s) 103 is authorized by the Secure **Digital** Content **Electronic** Distribution System 100. This is based on the fact that the Clearinghouse(s) 105 is the issuer of the certificates.

Alternately, the Clearinghouse(s) 105 would be able to successfully verify the **digital** signatures of the Transaction SC(s) 640 and Offer SC(s) 641 using the public key from the **Electronic Digital** Content Store(s) 103, but only if the entity signing the SC(s) has ownership of the associated private key. Only the **Electronic Digital** Content Store(s) 103 has ownership of the private key. Notice that the Clearinghouse(s) 105 does not need to have a local database of the **Electronic Digital** Content Store(s) 103. Since the store uses the Clearinghouse Public Key to sign the Transaction SC(s) 640 Offer SC(s) 641 public keys... ...watermarking instructions are done by the Clearinghouse(s) 105 after authenticity and the integrity check of the Order SC(s) 650, the validation of the **Electronic Digital** Content Store(s) 103, and the validation of the Store Usage Conditions 519 have been completed successfully. The Metadata SC(s) 620 portion of the... ...s) 109 is retrieved from the Order SC(s) 650. The new encrypted Symmetric Keys 623 are included in the Key Description part of the **License** SC(s) 660 that the Clearinghouse(s) 105 returns to the End-User Device(s) 109.

During the time of processing the Symmetric Keys 623... ...the Symmetric Keys 623, the watermarking instructions are modified and re-encrypted. The new watermarking instructions are included as one of the parts within the **License** SC(s) 660 that gets returned to the End-User Device(s) 109.

If all of the processing of the Order SC(s) 650 is successful, then the Clearinghouse(s) 105 returns a **License** SC(s) 660 to the End-User Device(s) 109. The End-User Device(s) 109 uses the **License** SC(s) 660 information to download the Content SC(s) 630 and access the encrypted Content 113 and metadata. The watermarking instructions are also executed... ...to successfully process the Order SC(s) 650, then an HTML page is returned to the End-User Device(s) 109 and displayed in an **Internet** browser window. The

HTML page indicates the reason that the Clearinghouse(s) 105 was unable to process the transaction.

In an alternate embodiment, if the user has purchased a copy of the Content II 3 prior to the release date set for the sale, the **License**(s) SC 660 is returned without the Symmetric Keys 623. The **License**(s) SC 660 is I 0 returned to the Clearinghouse(s) 105 on or after the release date to receive the Symmetric Keys 623. As... ...the End-User(s) resides, then the Clearinghouse(s) 105 insures that the transaction being processed is not violating any of those restrictions before transmitting **License** SC(s) 660 to the End-User Device(s) 109. The **Electronic Digital** Content Store(s) 103 is also expected to participate in managing the distribution of Content 113 to various countries by performing the same checks as the Clearinghouse(s) 105. The Clearinghouse(s) 105 does whatever checking that it can in case the **Electronic Digital** Content Store(s) 103 is ignoring the country specific rules set by the Content Provider(s) 1 01.

D. Audit Logs and Tracking
The Clearinghouse...during Content 113 purchase transactions and report request transactions. The information can be used for a variety of purposes such as audits of the Secure **Digital** Content **Electronic** Distribution System 100, generation of reports, and data mining.

The Clearinghouse(s) 105 also maintains account balances in Billing Subsystem 182 for the **Electronic Digital** Content Store(s) 103. Pricing structures for the **Electronic Digital** Content Store(s) 103 is provided to the Clearinghouse(s) 105 by the **digital** content labels. This information can include things like current specials, volume discounts, and account deficit limits that need to be imposed on the **Electronic Digital** Content Store(s) 103. The Clearinghouse(s) 105 uses the pricing information to track the balances of the **Electronic Digital** Content Store(s) 103 and insure that they do not exceed their deficit limits set by the Content Provider(s) 1 0 1.

The following operations are typically logged by the Clearinghouse(s) 105.

End-User Device(s) 109 requests for **License** SC(s) 660
Credit card authorization number when the Clearinghouse(s) 105 handles the billing
Dispersement of **License** SC(s) 660 to End-User Device(s) 109
Requests for reports
Notification from the End-User(s) that the Content SC(s) 630 and **License** SC(s) 660 were received and
validated
The following information is typically logged by the Clearinghouse(s) 105 for a **License** SC(s) 660.

Date and time of the request
Date and time of the purchase transaction
I 0 Content ID of the item being purchased
Identification of the Content Provider(s) 1 0 1

Store Usage Conditions 519
Watermarking instruction modifications
Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103
Identification of the **Electronic Digital** Content Store(s) 103
Identification of the End-User Device(s) 109
End-User(s) credit card information (if the Clearinghouse(s) 105 is handling... ...time of the request
Amount charged to the credit card
Content ID of the item being purchased
Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103
Identification of the **Electronic Digital** Content Store(s) 103
Identification of the End-User(s)
End-User(s) credit card information
Authorization number received from the clearer of the credit card
The following information is typically logged by the Clearinghouse(s) 105 when a **License** SC(s) 660 is sent to an End-User Device(s) 109.

Date and time of the request
Content ID of the item being purchased
Identification of Content Provider(s) IO 1
Usage Conditions 517
Transaction ID 535 that was added by the **Electronic Digital** Content Store(s) 103
Identification of the **Electronic Digital** Content Store(s) 103
Identification of the End-User(s)
The following information is typically logged when a report request is made.

Date and time... ...s) 105 using the information that the Clearinghouse(s) 105 0 logged during End-User(s) purchase transactions. Content Provider(s) 1 0 1 and **Electronic Digital** Content Store(s) 103 can request transaction reports from the Clearinghouse(s) 105 via a Payment Verification Interface 183 so they can reconcile their own... ...with the information logged by the Clearinghouse(s) 105. The Clearinghouse(s) 105 can also provide periodic reports to the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103.

The Clearinghouse(s) 105 defines a secure **electronic** interface which allows Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103 to request and receive reports. The Report Request SC(s) includes a certificate that was assigned by the Clearinghouse(s) 105 to the entity initiating the request. The Clearinghouse(s) 105 uses the certificate and the SC's **digital** signature to verify that the request originated from an authorized entity. The request also includes parameters, such as time duration, that define the scope of... ...version of this document.

F. Billing and Payment Verification
Billing of Content 113 can be handled either by the Clearinghouse(s) 105 or by the **Electronic Digital** Content Store(s) 103. In the case where the Clearinghouse(s) 105 handles the billing of the **electronic** Content 113, the **Electronic Digital** Content Store(s)

103 separates the End-User(s)' order into **electronic** goods and, if applicable, physical goods. The **Electronic Digital** Content Store(s) 103 then, notifies the Clearinghouse(s) 105 of the transaction, including the End-User(s)' billing information, and the total amount that needs to be authorized.

The Clearinghouse(s) 105 authorizes the End-User(s)' credit card and returns a notification back to the **Electronic Digital** Content Store(s) 103. At the same time the Clearinghouse(s) 105 is authorizing the End-User(s)' credit card, the **Electronic Digital** Content Store(s) 103 can charge the End-User(s)' credit card for any physical goods that are being purchased. After each **electronic** item is downloaded by the End-User Device(s) 109, the Clearinghouse(s) ...Device(s) 109 before the Content 1 1 3 is enabled for use at the End-User Device(s) 109.

In the case where the **Electronic Digital** Content Store(s) 103 handles the billing of the **electronic** Content 113, the Clearinghouse(s) 105 is not notified about the transaction until the End-User Device(s) 109 sends the Order SC(s) 650 to the Clearinghouse(s) 105. The Clearinghouse(s) 105 is still notified by the End-User Device(s) 109 after each **electronic** item is downloaded. When the Clearinghouse(s) 105 is notified it sends a notification to the **Electronic Digital** Content Store(s) 103 so that the **Electronic Digital** Content Store(s) 103 can charge the End-User(s)' credit card.

G, Retransmissions
The Secure **Digital** Content **Electronic** Distribution System 100 provides the ability to handle retransmissions of Content 113. This is typically performed by a Customer Service Interface 194. **Electronic Digital** Content Store(s) 103 provides a user interface that the End- User(s) can step through in order to initiate a retransmission. The End-User(s) goes to the **Electronic Digital** Content Store(s) 103 site where the Content 113 item was purchased in order to request a retransmission of the Content 1 1 3.

Retransmissions... ...a previously purchased Content 113 item because the Content 113 could not be downloaded or the Content 113 that was downloaded is not usable. The **Electronic Digital** Content Store(s) 103 determines whether the End-User(s) is entitled to do a retransmission of the Content 113. If the End-User(s) is entitled to a retransmission, then the **Electronic Digital** Content Store(s) 103 builds a Transaction SC(s) 640 that includes the Offer SC(s) 641 of the Content 1 13 item(s) being... ...109 to delete the scrambled key(s).

In the case where the Clearinghouse(s) 105 handles the financial settlement of Content 1 13 purchases, the **Electronic Digital** Content Store(s) 103 includes a flag in the Transaction SC(s) 640 that is carried forward to the Clearinghouse(s) 105 in the Order... ...End-User(s) for the purchase of the Content I 1 3.

VH1. CONTENT PROVIDER
A. Overview
The Content Provider(s) 101 in the Secure **Digital** Content **Electronic** Distribution System 100 is the **digital** content label or the entity who owns the **rights** to the Content

11 3. The role of the Content Provider(s) 101 is to prepare the Content I 1 3 for distribution and make information about the Content I 1 3 available to **Electronic** I 0 **Digital** Content Store(s) 103 or retailers of the downloadable **electronic** versions of the Content 113. To provide the utmost security and **rights** control to the Content Provider(s) 101, a series of tools are provided to enable the Content Provider(s) 1 0 1 to prepare and... ...domain and never exposed or accessible by unauthorized parties. This allows Content 113 to be freely distributed throughout a non-secure network, such as the **Internet**, without fear of exposure to hackers or unauthorized parties.

The end goal of the tools for the Content Provider(s) 1 0 1 is to... ...manages the required synchronization of processes.

Content Processing Tools 155 - A collection of tools to control Content 113 file preparation including Watermarking, Preprocessing (for an **audio** example any required equalization, dynamics adjustment, or re-sampling) encoding and compression.

Metadata Assimilation and Entry Tool 161 - A collection of tools **used** to gather **Content** 113 description information from the Database 160 of the Content Provider(s) and/or third party database or data import files and/or via operator interaction and provides means for specifying content Usage Conditions 517.

Also provided is an interface for capturing or extracting content such as **digital audio** content for CDS or DDP files. A Quality Control Tool enables to preview of prepared content and metadata. Any corrections needed to the metadata or... ...into SC(s).

Content Dispersement Tool (not shown) - Disperses SC(s) to designated distribution centers, such as Content Hosting Sitc(s) I I I and **Electronic Digital** Content Store(s) 103.

Content Promotions **Web** Site 156 - stores Metadata SC(s) 620 and optionally additional promotional material for download by authorized **Electronic Digital** Content Store(s) 103.

B. Work Flow Manager 154
The purpose of this tool is to schedule, track, and manage Content 113 processing activities. This...or as any of it's constitute processes may be distributed as an application program in a computer readable medium including but not limited to **electronic** distribution such as the **web** or on floppy diskettes, CD ROMS and removable hard disk drives.

Turning now to FIG. 8 is a block diagram of the major processes of... ...is entered to uniquely identify the product.

Optional ly, additional fields may be included to request manual entry of the information required to initiate the **audio** processing phase in parallel with the metadata acquisition. If not provided manually, this information can optionally be retrieved from default configuration settings or from the...the Database 160 of the Content Provider(s) IO 1 is

specified, the job is processed by the Automatic Metadata Acquisition Process 803. In a **music** embodiment, to properly schedule the product for **audio** processing, the product's genre and the desired compression levels are specified as well as the **audio** PCM or WAV filename(s). This information may be entered as part of the product selection process or selected via a customized query interface or **Web** browser function. Specification of this information enables the product to be scheduled for content processing.

The product selection user interface provides an option enabling the... ...Manual Metadata Entry Process 804 (see Automatic Metadata Acquisition Process 803 section for details on the Database Mapping Table).

If the required general information for **audio** processing and the specific information required for watermarking is specified, the job is queued for Watermarking Process 808 (the first phase of content processing).

if... ...status indicating the information that is missing.

If the status indicates that the filenarne of the Content 113, for example where the Content 113 is **audio** and the PCM or WAV file is missing, this may indicate that a capture (or **digital** extraction from **digital** media) is required. The **audio** processing functions require that the song files be accessible via a standard file system interface. If the songs are located on external media or a file system that is not directly accessible to the **audio** processing tools, the files are first be copied to an accessible file system. If the songs are in **digital** format but on CD or **Digital** Tape, they are extracted to a file system accessible to the **audio** processing tools. Once the files are accessible, the Work Flow Manager User Interface 700 is used to specify or select the path and filename for... ...Database 160 of the Content Provider(s) 101 to obtain the information necessary to process this Content 113. For example, if the Content 113 is **music**, the information needed to perform this query could be the album name or may be a UPC or a specific album or selection ID as... ...Action/Information Process 801.

6. Supervised Release Process 806
The Supervised Release Process 806 allows a quality check and validation of information specified for the **digital** content product. It does not have any dependencies. Comments previously attached to the job at any stage of the processing for this product can be...the usage conditions
the encryption keys used in the encryption stage of all quality levels for this product This last dependency requires that the associated **audio** objects completed the **audio** processing phase before the Metadata SC(s) 620 can be created. Upon completion of the Metadata SC(s) Creation Process 807, the job is queued... ...Process 81 1.

If third party providers of encoding tools do not provide a method to display the percentage of the Content 113, such as **audio**, that has been processed or a method to indicate the amount of Content 113 that has been encoded as a percentage of the entire selection of Content 113 selected, in FIG. I I there is shown a flow diagram 1100 of a

method to determine the encoding rate of **Digital** Content for the Content Preprocessing and Compression tool of FIG. 8. The method begins with the selection of the desired encoding algorithm and a bit... ...new rate factor RNEW. Calculating a new rate factor RNEw knowing the amount of time and the amount of Content 113 encodedis RNEW =(length of **Digital** Content encoded)/(amount of time), step II 08. The Content II 3 is encoded and the encoding status is displayed using the previously calculate rate...the song file remain available until after Content Quality Control Process 81 0.

II. Encryption Process 811
The Encryption Process 811 calls the appropriate Secure **Digital** Content **Electronic** Distribution **Rights** Management function to encrypt each of the watermarked/encoded song files. This process has no dependencies other than completion of all other **audio** processing. Upon completion of the Encryption Process 811 process, the job is queued for Content SC(s) Creation Process 812.

12. Content SC(s) Creation...quality level) tuple triggers an action).

C. Metadata Assimilation and Entry Tool
Metadata consists of the data describing the Content 1 13 for example in **music**, title of the recording, artist, author/composer, producer and length of recording. The following description is based upon Content 113 being **music** but it should be understood by those skilled in the art that other content types e.g., video, programs, multimedia, **movies**, and equivalent, are within the true scope and meaning of the present invention.

This Subsystem brings together the data the Content Provider(s) 101 provides to the **Electronic Digital** Content Store(s) 103 to help promote the sale of the product (e.g., for **music**, sample clips by this artist, history of this artist, list of albums on which this recording appears, genres associated with this artist and/or product End-User(s). The data is packaged into a Metadata SC(s) 620 and made available to the **Electronic Digital** Content Store(s) 103. To accomplish this, the following tools are provided.

Automatic Metadata Acquisition Tool
Manual Metadata Entry Tool
Usage Conditions Tool
Supervised Release... ...End- User(s) (e.g., composer, producer, sidemen, track length) and the types of promotional data the Content Provider(s) IO 1 provides to the **Electronic Digital** Content Store(s) 103 (e.g., for a **music** example, sample clips by this artist, a history of this artist, the list of albums on which this recording appears, genres associated with this artist... ...fields which can be I 0 optionally provided to the End-User Device(s) 109 and a sample set of data fields, targeted to the **Electronic Digital** Content Store(s) 103, that promote the artist, album, and/or single.

To extract the template data fields from the Database 160 of the Content... ...user the ability to implement the Usage Conditions Process 805 described above. The process of offering Content 113 for sale or rent (limited use), using **electronic** delivery, involves a series of business decisions. The Content Provider(s) 101 decides at which compression

level(s) the Content I 1 3 is made available. Then for each compressed encoded version of the Content I 1 3, one or more usage conditions are specified. Each usage condition defines the **rights** of the End-User(s), and any restrictions on the End- User(s), with regard to the use of the Content 1 13.

As part of Content Processing Tools 155, a set of usage conditions (End-User(s) **rights** and restrictions) is attached to the product.

A usage condition defines.

I . the compression encoded version of the Content I 1 3 to which this... ...for the purchase or the rental of the Content 1 1 3.

For a rental transaction.

the measurement unit which is used to limit the **term** of the rental (e.g., days, plays).

the number of the above units after which the Content I 1 3 will no longer play.

For... ...the period of time during which the purchase/rental transaction is allowed to occur (i.e., an End-User(s) can purchase/rent under the **terms** of this usage condition only after the beginning availability date and before the last date of availability).

5. the countries from which an End-User...Canada
watermarking std. std. std.

notifying events copy action none none
number of copies 1 0 0
onto what media MiniDisc not applicable not applicable
term of rental not applicable 14 days not applicable
price Price I Price 2 Price 3
countries USA and Canada USA and Canada USA and Canada
watermarking std. std. std.

notifying events copy action none none
number of copies 1 0 0
onto what media MiniDisc not applicable not applicable
term of rental not applicable 14 days not applicable
price Price I Price 2 Price 3
4. Parts of the Metadata SC(s) 620
Below are... ...everybodyJ
type of object (i.e., a single object or an array of objects)
object ID [dest: everybody;]
International Standard Recording Code (ISRC)
International Standard **Music** Number (ISMN)
usage conditions (sre: content provider; dest: EMS, end-user, Clearinghouse(s) 105)

purchased usage conditions (src: EMS; dest: end-user, Clearinghouse(s) 105) the set of usage conditions (consumer restrictions and **rights**) for the use of the object (sound recording)
an individual entry in the array of usage conditions
the compression encoded version of the Content II... ...allows for the purchase or the rental of the Content 1 13 for a rental transaction.

the measurement unit which is used to limit the **term** of the rental (e.g., days, plays).

the number of the above units after which the Content 1 1 3 will no longer play.

for... ...of time during which the purchase/rental transaction is allowed to occur (i.e., an I 0 End-User(s) can purchase/rent under the **terms** of this usage condition only after the beginning
availability date and before the last date of availability)
a pointer to the countries ftom which an... ...metadata 3 (src: content provider; dest: EMS, end-user)
optional info.

promotional material.

a pointer to artist promotion material
a URL to the artist's **web** site;
background description(s) of the artist(s);
artist-related interviews (along with format of the interview (e.g., text, **audio**, video));
reviews (along with format of the reviews (e.g., text, **audio**, video));
sample clips (and its format and compression level);
recent and upcoming concerts/appearances/events - their dates and locations;
a pointer to album promotion material
sample clip (and its format and compression level);
background description(s) of the producer, and/or the composer, and/or the **movie**/play/cast, and/or
the making of the album, etc.;
non-artist-related interviews (along with format of the interview (e.g., text, **audio**, video));
reviews (along with format of the reviews (e.g., text, **audio**, video));
genre(s);
single promotions:
I 0 sample clip (and its format and compression level)
background description(s) of the producer, and/or the composer, and/or the **movie**/play/cast, and/or the making of the single, etc.

reviews (along with format of the reviews (e.g., text, **audio**, video))
1 5 5. Supervised Release Tool
Supervised Release Tool provides a user the ability to implement the Supervised Release Process 806 described above. An...the retail channel.

D. Content Processing Tools
The Content Processing Tools 155 is actually a collection of software tools which are used to process the **digital** content file to create watermarked, encoded, and encrypted copies of the content. The tools makes use of industry standard **digital** content processing tools to allow pluggable replacement of watermarking, encoding and encryption technologies as they evolve. If the selected industry tool can be loaded via... ...C/C++ or any equivalent software. The Content Processing Tools 155 can be delivered by any computer readable means including diskettes, CDS or via a **Web** site.

1. Watermarking Tool
The Watermarking Tool provides a user the ability to implement the Watermarking Process 808 as described above. This tool applies copyright information of the Content 113 owner to the song file using **audio** Watermarking technology. The actual information to be written out is determined by the Content Provider(s) IO 1 and the specific watermarking technology selected. This... ...requirement on the Metadata Assimilation and Entry Tool 161 to assure that it has acquired this information prior to, for example, allowing the song's **audio** file to be processed. This song will not be available for **audio** processing until the watermarking information has been obtained.

The watermark is applied as the first step in **audio** processing since it is common to all encodings of the song created. As long as the watermark can survive the encoding technology, the watermarking process... ...Preprocessing and Compression Tool
The Preprocessing and Compression Tool provides a user the ability to implement the Preprocessing and Compression Process 809 as described above. **Audio** encoding involves two processes. Encoding is basically the application of a lossy compression algorithm against, for a **music** content example, a PCM **audio** stream. The encoder can usually be tuned to generate various playback bit stream rates based on the level of **audio** quality required. Fligher quality results in larger file sizes and since the file sizes can become quite large for high quality Content 113, download times... ...can become lengthy and sometimes prohibitive on standard 28,800 bps modems.

The Content Provider(s) 101 may, therefore, choose to offer a variety of **digital** content qualities for download to appease both the impatient and low bandwidth customers who don t want to wait hours for a download and the... ...to the compression algorithm. To allow for more efficient compression with less loss of fidelity or to prevent drastic dropout of some frequency ranges, the **digital** content may sometimes require adjustments to equalization levels of I 0 certain frequencies or adjustments to the dynamics of the recording. The content preprocessing requirements... ...compression tools, these preprocessing functions are part of the encoding process. With others, the desired preprocessing is performed prior to the compression.

Besides the downloadable **audio** file for sale, each song also has a Low Bit Rate (LBR) encoded clip to allow the song to be sampled via a LBR streaming... ...compression. The front end Encoding Tool may have a synchronization requirement with the Metadata Assimilation and Entry Tool 161, for example if the content is **music**, and if it is

determined that the song's genre is acquired from the Database 160 of the Content Provider(s) prior to performing any **audio** preprocessing. This depends on the encoding tools selected and how indeterminate the genre for the song is. If the Content Provider(s) 101 varies the... ...present invention. The process starts with reading an identifier from the media the Content Provider(s) 101 is examining. One example of content in an **audio** CD embodiment. In an **audio** CD embodiment, the following codes may be available Universal Price Code (UPC), International Standard Recording Code (ISRC), International Standard **Music** Number (ISMN). This identifier is read in the appropriate player for the content, for example an **audio** CD Player for **audio** CD, DVD player for DVD **movie**, DAT recorder for DAT recording and equivalent, step 1201. Next this Identifier is used to index a Database 160 for the Content Provider(s) 101... ...3 and the metadata related to it. In step 1204, the additional information retrieved is used to start the Work Flow Manager 154 for creating **electronic** Content 113. It should be understood, that several selections of media, such as several **audio**- CDS, can be queued up so as to enable the Automatic Metadata Acquisition Tool to create a series of Content 113 for **electronic** distribution. For example, all the Content 113 could be created from a series of CDS or even selected tracks from one or more CDS examined... ...Preprocessing and Compression parameters of the Preprocessing and Compression Tool of FIG. 8 according to the present invention. In this embodiment. the Content 113 is **music**. In step 1301, **music** (Content 113) is selected to be encoded in Content Processing Tools 155. The genre of the **music** selected is determined, step 1302.

This can be entered manually or by using other meta data available, such as the additional data retrieved from the process described in FIG. 12. The **audio** compression level and **audio** compression algorithms selected are than examined, step 1303. Next, a lookup is made by genre, compression settings and compression algorithms of what compression parameters should 620 and multiple Content SC(s) 630 for each song. For example, if the content is **music**, each of the **audio** files created during **audio** processing for the various quality levels of the full song is packed into separate Content SC(s) 630. The **audio** file created for the sample clip is passed as a metadata. file to be included in the Metadata SC(s) 620.

F. Final Quality Assurance... ...101 can choose to perform quality assurance as each major step is completed to prevent excessive rework later or may choose to wait until all **audio** preparation processes are complete and perform quality assurance on everything at once. If the latter is chosen, quality assurance is performed at this point upon completion of the creation of the SC(s). This tool allows each SC(s) for the song to be opened, examined, and the **audio** played.

Any problem discovered, even minor text changes requires that the SC(s) be rebuilt due to internal security features of SC(s). To avoid... ...101 to prepare content in advance of their scheduled release date and hold them until they wish to release them e.g., a new song, **movie** or game. The SC(s) can also control access to Content I 1 3 based on a defined release date so there is no requirement... ...via FTP to the designated Content Hosting Site(s) I 1 1. The Metadata SC(s) 620 is transferred via FTP to the Content Promotions **Web** Site 156. Here the SC(s) are staged to a new Content 1 13 directory

until they can be processed and integrated into the Content Promotions **Web** Site 156.

FIG. 17 is a flow diagram of an alternate embodiment to automatically retrieve additional information for the Automatic Metadata Acquisition Tool of FIG... ...Manual Metadata Entry 803. Since, many of the usage conditions can be automatically filled-in during the Automatic Metadata Acquisition 803 step.

H, Content Promotions **Web** Site
To most effectively disperse information on what the Content Provider(s) 101 is making available for sale via **digital** download, and to get the necessary files to the **Electronic Digital** Content Store(s) 103 to enable it to make this Content 113 available for download to its customers, each Content Provider(s) 101 should have a secure **web** site housing this information. This is similar to the method used today by some Content Provider(s) 101 to make promotional content available to their... ...others with a need for this information. In the case where this type of service already exists, an additional section can be added to the **web** site where **Electronic Digital** Content Store(s) 103 can go to see a list of the content available for sale ...The Content Provider(s) 1 0 1 has complete control over the design and layout of this site or can choose to use a turnkey **web** server solution provided as part of the toolkit for Secure **Digital** Content **Electronic** Distribution System I 00. To implement their own design for this service, the Content Provider(s) 1 0 1 need only provide links to the Metadata SC(s) 620 for **Electronic Digital** Content Store(s) 103 who access their site. This is accomplished using the toolkit for the Secure **Digital** Content **Electronic** Distribution System 100. The selection process and what information is shown is the discretion of the Content Provider(s) 101.

Metadata SC(s) 620 received into a new content directory via FTP from the Content Dispersement Tool is processed by the Content Promotions **Web** Site 156. These containers can be opened with the SC(s) Preview Tool to display or extract information from the container. This information can then be used to update HTML **Web** pages and/or add information to a searchable database maintained by this service. The SC(s) Preview Tool is actually a subset of the **Content** Acquisition Tool **used** by the **Electronic Digital** Content Store(s) 103 to open and process Metadata SC(s) 620. See the Content Acquisition Tool section for more details. The Metadata SC(s) 620 file should then be moved to a permanent directory maintained by the Content Promotions **Web** Site 156.

Once the Metadata SC(s) 620 has been integrated into the Content Promotions **Web** Site 156, its availability is publicized. The Content Provider(s) 101 can send a notification to all subscribing **Electronic Digital** Content Store(s) 103 as each new Metadata SC(s) 620 is added to the site or can perform a single notification daily (or any defined periodicity) of all Metadata SC(s) 620 added that day (or period). This notification is performed via a standard HTTP exchange with the **Electronic Digital** Content Store(s) 103 **Web** Server by sending a defined CGI string containing parameters referencing the Metadata SC(s) 620 added. This message is handled by the Notification Interface Module of the **Electronic Digital** Content Store(s) 103 which is described later.

1. Content Hosting

The Entertaim-nent Industry produces thousands of content titles, such as CDS, **movies** and games every year, adding to the tens of thousands of content titles that are currently available. The Secure **Digital** Content **Electronic** Distribution System 100 is designed to support all of the content titles available in stores today.

The numbers of content titles that the Secure **Digital** Content **Electronic** Distribution System 100 may eventually download to customers on a daily basis is in the thousands or tens of thousands. For a large number of... ...The system also supports customers all over the world. This requires overseas sites to speed delivery to the global customers.

Content hosting on the Secure **Digital** Content **Electronic** Distribution System 100 is designed to allow the Content Provider(s) 1 01 to either host their own Content 1 13 or share a cornmon facility or a set of facilities.

Content hosting on the Secure **Digital** Content **Electronic** Distribution System 100 consists of multiple Content Hosting Site(s) 1 1 1 that collectively contain all of the Content 1 1 3 offered by the Secure **Digital** Content **Electronic** Distribution System 100 and several Secondary Content Sites (not shown) that contain the current hot hits offered bythe Content Provider(s) 101. Thenumber of Content... ...Hosting Site 1 1 1 with or without additional Secondary Content Sites. This allows them to build their own scalable distributed system. In another embodiment, **Electronic Digital** Content Store(s) 103 can also act as Content Hosting Site(s) III for certain Content 1 1 3. This embodiment requires a special financial agreement between the **Electronic Digital** Content Store(s) 103 and the Content Provider(s) 1 0 1.

1 . Content Hosting Sites

Content 1 1 3 is added to the Content... ...indicates the URL locating the Content SC(s) 630 for this Content 113. This URL corresponds to a Content Hosting Site(s) I I 1. **Electronic Digital** Content Store(s) 103 can override this URL if allowed by the Content Provider(s) IO 1 in the Offer SC(s) 64 1. The... ...to download the Content SC(s) 630.

The End-User Device(s) 109 initiates the request for a Content SC(s) 630 by sending the **License** SC(s) 660 to the Content Hosting Site(s) 1 1 1. This is the same **License** SC(s) 660 returned by the Clearingbouse(s) 105. The **Digital** Signature of the **License** SC(s) 660 can be verified to determine if it is a valid **License** SC(s) 660. If it is a valid **License** SC(s) 660 either the download is initiated, or the download request may be redirected to another Content Hosting Site(s) 1 1 1.

2. Content Hosting Site(s) 1 1 1 provided by the Secure **Digital** Content **Electronic** Distribution System I 00 For the Secure **Digital** Content **Electronic** Distribution System I 00 the decision of which site should be used to download the Content 113 is made by the primary content site that... ...make this decision.

Are there secondary content sites that host the Content 1 13 requested? (The majority of Content 1 13 offered by the Secure **Digital** Content **Electronic** Distribution System I 00

is only located at primary sites); Where is the End-User Device(s) 109 geographically located? (This information can be obtained... ...the End-User Device(s) 109, analysis and verifications are performed on the End-User's request. A database is kept of all of the **License** SC IDs that have been **used** to download **Content** 113. This database can be checked to ensure that the End-User Device(s) 109 only makes one request for each piece of Content 113... ...the amount of activity on the sites and whether a site is down for maintenance.

The only interface to the Content Hosting Router is the **License** SC(s) 660 that is sent by the End-User Device(s) 109 when Content 113 is required to be downloaded. The **License** SC(s) 660 includes information that indicates the user is allowed to download the Content I 1 3.

Secondary Content Sites
The Secondary Content Sites (not shown) host the popular Content 113 of the Secure **Digital** Content Distribution System 100. These sites are geographically dispersed across the world and are located near Network Access Points (NAPs) to improve download times. These sites are added to the system as demand on the primary
Content Hosting Site(s) I 1 1 nears maximum capacity
IX. **ELECTRONIC DIGITAL** CONTENT STORE(S)
A. Overview - Support for Multiple **Electronic Digital** Content Store(s) 103 **Electronic Digital** Content Store(s) 103 are essentially the retailers. They are the entities who market the Content I 1 3 to be distributed to the customer. For distribution of Content 1 1 3, this would include **Digital** Content Retailing **Web** Sites, **Digital** Content Retail Stores, or any business who wishes to get involved in marketing **electronic** Content 113 to consumers. These businesses can market the sale of **electronic** Content 113 only or can choose to just add the sale of **electronic** goods to whatever other merchandise they currently offer for sale.

Introduction of downloadable **electronic** goods into the service offering of the **Electronic Digital** Content Store(s) 103 is accomplished via a set of tools developed for the **Electronic Digital** Content Store(s) 103 as part of the Secure **Digital** Content **Electronic** Distribution System I 00.

These tools are used by the **Electronic Digital** Content Store(s) 103 to.

acquire the Metadata SC(s) 620 packaged by the Content Provider(s) 1 0 1
extract Content 1 13 from... ...the status of each download
handle status notifications and transaction authentication requests
perform account reconciliation
The tools are designed to allow flexibility in how the **Electronic Digital** Content Store(s) 103 wishes to integrate sale of downloadable **electronic** Content 113 into its service. The tools can be used in such a way as to request that all financial settlements for downloadable Content 113 purchased be handled by the Clearinghouse(s) 105 although this is not required. These tools also enable **Electronic Digital** Content Store(s) 103 to completely service their customers and handle the financial transactions themselves,

including providing promotions and special offers. The tools enable the **Electronic Digital** Content Store(s) 103 to quickly integrate the sale of downloadable Content 113 into its existing services. In addition, the **Electronic Digital** Content Store(s) 103 is not required to host the downloadable Content 113 and does not have to manage its dispersement. ...function is performed by the Content Hosting Site(s) I I 1 selected by the Content Provider(s) 1 0 1.

The tools for the **Electronic Digital** Content Stores(s) 103 are implemented in Java in the prefdred embodiment but other programming languages such as C/C++, Assembler and equivalent can be used. It should be understood that the tools described below for the **Electronic Digital** Content Stores(s) 103 can run on a variety of hardware and software platforms. The **Electronic Digital** Content Stores(s) 103 as a complete system or as any of it's constitute components may be distributed as an application program in a computer readable medium including but not limited to **electronic** distribution such as the **web** or on floppy diskettes, CD ROMS and removable hard disk drives.

In another embodiment, the components of the **Electronic Digital** Content Stores(s) 103 is part of a programmer's software toolkit. This toolkit enables predefined interfaces to the components of the generic **Electronic Digital** Content Stores(s) 103 components and tools discussed below. These predefined interfaces are in the form of APIs or Application Programming Interfaces. A developer using these APIs can implement any of the functionalityofthecomponentsfromahigh-levelapplicationprogram. ByprovidingAPIstothesecomponents,a program mer can quickly develop a customized **Electronic Digital** Content Stores(s) 103 without the need to re-created these functions and resources of any of these components.

Electronic Digital Content Store(s) 103 are not limited to **Web** based service offerings. The tools provided are used by all **Electronic Digital** Content Store(s) 103 wishing to sell downloadable **electronic** Content 113 regardless of the transmission infrastructure or delivery mode used to deliver this Content 113 to End-User(s).

Broadcast services offered over satellite and cable infrastructures also use these same tools to acquire, package, and track **electronic** Content 113 sales. The presentation of **electronic** merchandise for sale and the method in which these offers are delivered to the End-User(s) is the main variant between the broadcast based service offering and the point-to-point interactive **web** service type offering.

1 5
B. Point-to-Point **Electronic Digital** Content Distribution Service
Point-to-Point primarily means a one-to-one interactive service between the **Electronic Digital** Content Store(s) 103 and the End-User Device(s) 109. This typically represents an **Internet web** based service provided via telephone or cable modern connection. Networks other than the **Internet** are supported in this model as well, as long as they conform to the **Web** Server/Client Browser model. FIG. 9 is a block diagram illustrating the major tools, components and processes of an **Electronic Digital** Content Store(s) 103.

1 . Integration Requirements

The Secure **Digital** Content **Electronic** Distribution System 100 not only creates new **online** businesses but provides a method for existing businesses to integrate the sale of downloadable **electronic** Content 113 to their current inventory. The suite of tools provided to the **Electronic Digital** Content Store(s) 103 simplify this integration effort. The Content Acquisition Tool 171 and SC(s) Packer Tool 153 provides a method for the **Electronic Digital** Content Store(s) 103 to acquire information from the participating Content Provider(s) 101 on what they have available for sale and to create the... ...driven and can be largely automated and is executed only to integrate new Content 1 1 3 into the site.

The tools for the Secure **Digital** Content **Electronic** Distribution have been designed to allow integration of sale of **electronic** downloadable Content 113 into typical implementations of **web** based **Electronic Digital** Content Store(s) 103 (i.e. Columbia House **online**, **Music** Boulevard, @Tower) and equivalent with minimal change to their current Content 1 13 retailing paradigm. Several methods of integration are possible and in the preferred embodiment, the **Electronic Digital** Content Store(s) 103 provides support for all product searches, previews, selections (shopping cart), and purchases. Each **Electronic Digital** Content Store(s) 103 establishes customer loyalty with its customers and continues to offer its own incentives and market its products as it does today. In the Secure **Digital** Content **Electronic** Distribution System I 00, it would simply need to indicate which products in its inventory are also available for **electronic** download and allow its customers to select the **electronic** download option when making a purchase selection. -In another embodiment, the customer's shopping cart could contain a mixture of **electronic** (Content 113) and physical media selections. After the customer checks out, and the **Electronic Digital** Content Store(s) 103 has completed the financial settlement and logged or notified its shipping and handling functions to process the physical merchandise purchased, the commerce handling function of the **Electronic Digital** Content Store(s) 103 then calls the Transaction Processor Module 175 to handle all **electronic** I 0 downloads. It simply passes the required information and all processing from that point on is handled by the toolset for the Secure **Digital** Content **Electronic** Distribution System 100. In another embodiment, other methods of transaction handling are also possible using tools for the Secure **Digital** Content **Electronic** Distribution System 100 to handle the financial settlement should the **Electronic Digital** Content Store(s) 103 wish to sell downloadable merchandise only or to segregate the financial settlement of physical and downloadable merchandise.

To handle the downloading of merchandise, the **Electronic Digital** Content Store(s) 103 is given a Product ID (not shown) for each downloadable product that it acquires from the Content Promotions **Web** Site 156 for the Content Provider(s) 101. This Product ID is associated to a customer's purchase selection to the downloadable product. The Product ID is what the **Electronic Digital** Content Store(s) 103 passes to the Transaction Processor Module 175 to identify the product that the user has purchased. The SC(s) (Offer SC(s) 641) that were created to describe the products, are isolated from the **Electronic Digital** Content Store(s) 103 and kept in an Offer Database 181 in an effort to simplify management of these objects and make their existence transparent to the

Electronic Digital Content Store(s) 103.

The Transaction Processor Module 175 and other additional functions are provided as **web** server side executables (i.e. CGI and NSAPI, ISAPI callable fiinctions) or simply APIs into a DLL or C object library. These functions handle run time processing for End-User(s) interactions and optional interactions with the Clearinghouse(s) 105. These functions interact with the **web** server's commerce services to create and download to the End-User Device(s) 109 the files necessary to initiate the Content 113 download process... ...also handle optional interactions to provide authorizations and accept notifications of completion of activities.

An Accounting Reconciliation Tool 179 is also provided to assist the **Electronic Digital** Content Store(s) 103 in contacting the Clearinghouse(s) 105 to reconcile accounts based on its own and the transaction logs of the Clearinghouse(s) 105.

2. Content Acquisition Tool 171
The Content Acquisition Tool 171 is responsible for interfacing with the Content Promotions **Web** Site 156 to preview and download Metadata SC(s) 620. Since the Content Promotions site is a standard **web** site, a **web** browser is used by the **Electronic Digital** Content Store(s) 103 to navigate this site. The navigation features varies based on the site design of the Content Provider(s) 101. Some sites... ...from. All sites include the selection of Metadata SC(s) 620 containing all the promotional and descriptive information of a song or album. .

Alternatively, the **Electronic** Store(s) 103 may subscribe to content updates and receive updates automatically via FTP.

I 0
Viewing Metadata
The Content Acquisition Tool 171 is a **web** browser helper application which launches whenever a Metadata SC(s) 620 link is selected at the Content Promotions **Web** Site 156. Selection of the SC(s) causes it to be downloaded to the **Electronic Digital** Content Store(s) 103, and launch the helper application. The Content 1 5 Acquisition Tool 171 opens the Metadata SC(s) 620 and display the non-encrypted information contained therein.

Displayed information includes Extracted Metadata 173, for a **music** example, the graphic image(s) associated with the song and the information describing the song, a preview clip of the song can also be listened to if included in the Metadata SC(s) 620. In an example where the Content 113 is **music**, promotional information about the song or album, the album title, and the artist is also shown if provided by the Content Provider(s) 1 0... ...as the song and the lyrics and whatever other metadata the Content Provider(s) 101 wishes to protect, is not accessible to the Retail Content **Web** Site 180.

In another embodiment, the Content Provider(s) IO 1 provides optimal promotional content for a fee. In this embodiment such promotional content is... ...in the Metadata

SC(s) 620. Financial settlement to open this data can be handled via the Clearinghouse(s) 105 with the account for the **Electronic Digital** Content Store(s) 103 being charged the designated fee.

Extracting Metadata.

Besides the preview capabilities, this tool provides two additional features: metadata extraction and preparation of an Offer SC(s) 641. Selection of the metadata extraction option prompts the **Electronic Digital** Content Store(s) 103 to enter the path and filenames to where the metadata is to be stored. Binary metadata such as graphics and the **audio** preview clip is stored as separate files. Text metadata is stored in an ASCII delimited text file which the Retail Content **Web** Site 180 can then import into its database. A table describing the layout of the ASCII delimited file is also be created in a separate... ...One important piece of information provided in the extracted data is the Product ID. This Product ID is what the commerce handling function for the **Electronic Digital** Content Store(s) 103 needs to identify to the Transaction Processor Module 175 (for more information refer to Transaction Processing section), the Content 113 that... ...to properly retrieve the appropriate Offer SC(s) 641 from the Offer Database 181 for subsequent download to the End-User Device(s) 109.

The **Electronic Digital** Content Store(s) 103 has full control over how it presents the offer of downloadable Content 113 on its site. It only needs to retain a cross reference of the Content 113 being offered to this Product ID to properly interface with the tools for the Secure **Digital** Content **Electronic** Distribution System I 00. Providing this information here, allows the **Electronic Digital** Content Store(s) 103 to integrate this product or Content 113 into its inventory and sales pages (database) in parallel with the Offer SC(s... ...process since both processes uses the same Product ID to reference the product. This is described further below.

Offer SC(s) Creation Packer 153
The **Electronic Digital** Content Store(s) 103 is required to create an Offer SC(s) 641 describing the downloadable Content 113 that is for sale. Most of the in this tool for the **Electronic Digital** Content Store(s) 103
prompting for additional required inputs or selections as defined by the Offer SC(s) Template in the
Metadata SC(s) 620... ...later) on the End-User Device(s) 109 is kept in the Metadata SC(s) 620. Other promotional metadata that was only used by the **Electronic Digital** Content Store(s) 103 as input to his **web** service database is removed from the Metadata SC(s) 620. **Rights** management information provided by the Content Provider(s) 101, such as watermarking instructions, encrypted Symmetric Keys 623, and Usage Conditions 517 defining the permitted uses of the object, are also retained.

This stripped down Metadata SC(s) 620 is then included in the Offer SC(s) 641. The **Electronic Digital** Content Store(s) 103 also attaches its own Usage Conditions called Store Usage Conditions 519 or purchase options to the Offer SC(s) 64 1. This can be accomplished interactively or automatically through a set of defaults.

If configured to be processed interactively, the **Electronic Digital** Content Store(s) 103 is prompted with the set of permitted object Usage Conditions 517 as defined by the Content Provider(s) I 01. He... ...option(s) he wishes to offer to his customers. These now become the new Usage Conditions or Store Usage Conditions 519. To process automatically, the **Electronic Digital** Content Store(s) 103 configures a set of default purchase options to be offered for all Content 113. These default options are automatically checked against... ...Database 181 and is indexed with the Product ID pre-assigned in the Metadata SC(s) 620. This Product ID is used later by the **Electronic Digital** Content Store(s) 103 to identify the downloadable Content 113 being purchased by a customer when interfacing with the Offer Database 181 to retrieve the... ...s) 641 for packaging and transmittal to the End-User(s). See the Transaction Processor Module 175 section for more details.

In another embodiment, the **Electronic Digital** Content Store(s) 103 hosts the Content SC(s) 641 at his site.

This embodiment requires changes to the Offer SC(s) 641 such as the replacement of the URL of the Content I 0 Hosting Site(s) I 1 1 with the URL of the **Electronic Digital** Content Store(s) 103.

3. Transaction Processing Module 175
Electronic Digital Content Store(s) 103 directs billing to Clearinghouse(s) 105. Alternatively, the **Electronic Digital** Content Store(s) 103 may request financial clearance direct from the Clearinghouse(s) 105.

There are two basic modes for processing End-User(s) purchase requests for downloadable Content 113. If the **Electronic Digital** Content Store(s) 103 does not wish to handle the financial settlement of the purchase and has no special promotions or incentives governing the sale... ...pricing information included in the metadata. Also included in the Offer SC(s) 641 is a special HTML offer page presenting the purchase options with **terms** and conditions of the sale. This page is built from a template created when the Offer SC(s) 641 was built. When the End- User... ...this form may contain the fields needed to use the End-User(s)' credit information or industry standard local transaction handler.

An embodiment where the **Electronic Digital** Content Store(s) 103 handles billing is now described. The more typical modc of handling purchase requests is to allow the **Electronic Digital** Content Store(s) 103 to process the financial settlement and then submit the download authorization to the End-User(s). This method allows-the **Electronic Digital** Content Store(s) 103 to integrate sale of downloadable Content 113 with other merchandise offered for sale at his site, allows batch processing of purchase requests with only one consolidated charge to the customer (via a shopping cart metaphor) instead of individual charges for each download request, and allows the **Electronic Digital** Content Store(s) 103 to directly track his customers buying patterns and offer special promotions and club options. In this environment, the offer of

downloadable... ...which get added to a shopping cart when selected by the End-User(s) and get processed and financially settled as is done in the **Electronic Digital** Content Store(s)' 103 current shopping model. Once the financial settlement is completed, the commerce handling process of the **Electronic Digital** Content Store(s) 100 then calls the Transaction Processor Module 175 to complete the transaction.

Transaction Processor Module 175
The role of the Transaction Processor **Web** Server as the response to the purchase submission. The Transaction Processor Module 175 requires three pieces of information from the commerce handling process of the **Electronic Digital** Content Store(s) 103: the Product IDs for the Content 113 purchased, Transaction Data 642, and an HTML page or CGI URL acknowledging the purchase settlement.

The Product ID is the value provided to the **Electronic Digital** Content Store(s) 103 in the Metadata SC(s) 620 associated to the Content 113 just sold. This Product ID is used to retrieve the... ...SC(s) 641 from the Offer Database 181.

The Transaction Data 642 is a structure of information provided by the transaction processing function of the **Electronic Digital** Content Store(s) 103 which is later used to correlate the Clearinghouse(s) 105 processing with the financial settlement transaction performed by the **Electronic Digital** Content Store(s) 103 and to provide user identity information to be included in the watermark of the Content 113 downloaded to the End-User... ...the Clearinghouse(s) 105 receives a valid Order SC(s) 650, it logs a transaction indicating the Content 1 1 3 that was sold, which **Electronic Digital** Content Store(s) 103 sold it and the associated Transaction Data 642 including the End-User's Name and a Transaction ID 535. The Transaction ID 535 provides a reference to the financial settlement transaction. This information is later returned by the Clearinghouse(s) 105 to the **Electronic Digital** Content Store(s) 103 for use in reconciling its accounts with the billing statements received from the Content Provider(s) 101 (or his agent). The Clearinghouse Transaction Log 178 can be **used** by the **Content** Provider(s) 101 to determine what Content 113 of his has been sold and enables him to create a bill to each **Electronic Digital** Content Store(s) 103 for royalties owed him. Other **electronic** means besides billing can alternatively be used to settle accounts between the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103.

The information provided in the Transaction SC(s) 640 and the security and integrity of the Transaction SC(s) 640 provide... ...the purchase transaction is valid and thus no further validation is required prior to the logging of this sale by the Clearinghouse(s) 105. The **Electronic Digital** Content Store(s) 103, however, has the option to request authentication before its accounts are charged (transaction logged at the Clearinghouse(s) 105 indicating to the Content Provider(s) 101 that this **Electronic Digital** Content Store(s) 103 has collected money for the sale of this Content 113). This request for authentication/notification is indicated by a flag in the Transaction Data 642. In this scenario, the Clearinghouse(s) 105 contacts the **Electronic Digital** Content Store(s) 103 and receive authorization ftom the **Electronic Digital** Content Store(s) 103 before the charge to his account and the release of the encryption Key 623.

The Transaction ID 535 is passed to the **Electronic Digital** Content Store(s) 103 from the Clearinghouse(s) 105 as part of this authentication request to enable the **Electronic Digital** Content Store(s) 103 to associate this request to a prior transaction performed with the End-User(s). This Transaction ID 535 can be any unique value the **Electronic Digital** Content Store(s) 103 wishes to use and is solely for its benefit.

The Transaction Data 642 also contains a customer name. This name can... ...of the purchase form filled out by the user when making his purchase, or from information logged previously during some user registration process with the **Electronic Digital** Content Store(s) 103, or the official name obtained from credit card information associated with the card used in this transaction. This name is later included in the I 0 **License** Watermark 527.

The Transaction Data 642 also contains the Store Usage Conditions 519 purchased by the End-User(s).

This information is included in the **License** Watermark 527 and used by the End- User Device(s) 109 in Copy and Play Control.

The final parameter required by the Transaction Processor Module 175 is the HTML page or CGI URL acknowledging the purchase settlement. The purpose of this is to allow the **Electronic Digital** Content Store(s) 103 to respond to the End-User(s) with an acknowledgment of the financial settlement and whatever other information he wishes to... ...the Transaction SC(s) 640 is received and processed.

The Transaction SC(s) 640 is the HTTP response to the End-User(s) from the **Electronic Digital** Content Store(s) 103 after processing the purchase submission. Sending a SC(s) as the direct HTTP response forces the automatic loading on the End... ...use by the Notification Interface Module 176 and the Account Reconciliation Tool 179.

4. Notification Interface Module 176
The Notification Interface Module 176 is a **Web** Server side executable routine (CGI or function callable by NSAPI, ISAPI or equivalent). It handles optional requests and notifications from the Clearinghouse(s) 105, the End-User Device(s) 109, the Content Hosting Site(s) 1 1 1, and the Content Provider(s) IO 1. The events that the **Electronic Digital** Content Store(s) 103 can optionally request notification for are.

Notification from the Clearinghouse(s) 105 that the End-User Device(s) 109 requested an... ...Clearinghouse(s) 105 is releasing the encryption Key 623 for the specified Content 113. This notificatim can optimally be configured to require authentication from the **Electronic Digital** Content Store(s) 103 prior to the encryption Key 623 being sent to the End-User Device(s) 109.

Notification from the Content Hosting Site... ...been sent to the End-User Device(s) 109.

Notification from the End-User Device(s) 109 that the Content SC(s) 630 and the **License** SC(s) 660 have been received and successfully used to process the Content 113 or was found to be corrupt.

Notification from the Content Provider(s) 101 that new Content 113 has been placed in the Content Promotions **Web** Site 156.

None of these notifications are a required step in the Secure **Digital** Content **Electronic** Distribution System flows I 00 but are provided as options to allow the **Electronic Digital** Content Store(s) 103 the opportunity to close its records on the satisfaction of completion of the sale. It also provides information that may be needed to handle customer service requests by letting the **Electronic Digital** Content Store(s) 103 know what functions have transpired since financial settlement of the transaction or what errors occurred during an attempt to complete the... ...from the Clearinghouse(s) 105 through the Customer Service Interface 184 as needed.

Frequency of notification of new Content 113 available at the Content Promotions **Web** Site 156 is determined by the Content Provider(s) 101. Notification may be provided as each new Metadata SC(s) 620 is added or just... ...all new Metadata SC(s) 620 added that day.

All of these notifications result in entries being made to the Transaction Log 178. If the **Electronic Digital** Content Store(s) 103 wishes to perform his own processing on these notifications, he can intercept the CGI call, perform his unique function and then... ...to compare the Transaction Log 178 with the log of the Clearinghouse(s) 105. This is an optional process which is available to help the **Electronic Digital** Content Store(s) 103 feel comfortable with the accounting for the Secure **Digital** Content **Electronic** Distribution System 100.

In another embodiment, this tool can be updated to provide **electronic** funds transfers for automated periodic payments to the Content Provider(s) 101 and the Clearinghouse(s) 105. It can also be designed to automatically process payments upon reception of an **electronic** bill from the Clearinghouse(s) 105 after reconciling the bill against the Transaction Log 178.

C. Broadcast **Electronic Digital** Content Distribution Service
Broadcast primarily refers to a one to many transmission method where there is no personal interaction between the End-User Device(s) 109 and the **Electronic Digital** Content Store(s) 103 to customize on-demand viewing and listening. This is typically provided over a **digital** satellite or cable infrastructure where the Content II 3 is preprogrammed so that all End-User Device(s) 109 receive the same stream.

A hybrid model can also be defined such that an **Electronic Digital** Content Store(s) 103 provides a **digital** content service organized in such a way that it can offer both a **web** distribution interface via an **Internet** connection as well as a higher bandwidth satellite or cable distribution interface via a broadcast service, '%kith a great deal of commonality to

the site design. If the IRD backchannel serial interface were connected to the **web**, and the IRD supported **web** navigation, the End-User(s) could navigate the **digital** content service in the usual way I 0 via the backchannel **Internet** interface, previewing and selecting Content 1 1 3 to purchase. The user can select high quality downloadable Content 113, purchase these selections, and receive the required **License** SC(s) 660 all via an **Internet** connection and then request delivery of the Content 113 (Content SC(s) 630) over the higher bandwidth broadcast interface. The **Web** service can indicate which Content 113 would be available for download in this manner based on the broadcast schedule or could build the broadcast streams based totally on purchased Content 113. This method would allow a **Web** based **digital** content service to contract with a broadcast facility to deliver high quality Content 113 to users equipped with the proper equipment making a limited number... ...specific Content 113 (e.g. songs or CDS) available daily in this manner and the entire catalog available for download in lower quality via the **web** interface.

Other broadcast models can be designed where there is no **web** interface to the End-User Device(s) 109. In this model, promotional content is packaged in specially formatted **digital** streams for broadcast delivery to the End-User Device(s) 109 (i.e. IRD) where special processing is performed to decode the streams and present... ...End-User Device(s) 109 to the Clearinghouse(s) 105 and would utilize SC(s) to perform all data exchange. The toolset provided to the **Electronic Digital** Content Store(s) 103 has been architected and developed in such a way that most of the tools apply to both a point-to-point **Internet** service offering as well as a broadcast satellite or cable offering.

The tools used by a **Digital** Content **Web** Site **Electronic Digital** Content Store(s) 103 to acquire and manage Content 113 as well as prepare SC(s) is also used by a satellite based **Electronic Digital** Content Store(s) 103 to manage and prepare Content 113 for distribution on a broadcast infrastructure. The SC(s) distributed over a **Web** service are the same as those distributed over a broadcast service.

X. END-USER DEVICE(S) 109
The applications in the End-User Device(s) 109 for the Secure **Digital** Content **Electronic** Distribution System 100 perform two main functions: first the SC(s) processing and copy control; and second playback of encrypted Content 113. Whether the End-User Device(s) 109 is a Personal Computer or a specialized **electronic** consumer device, it has to be capable of performing these base functions. The End-User Device(s) 109 also provides a variety of additional features and -functions like creating play lists, managing the **digital** content library, displaying information and images during content playback, and recording to external media devices. These functions vary based on the services these applications are... ...FIG. 10, shown is the major components and processes and End-User Device(s) 109 Functional Flow. The applications designed to support a PC based **web** interface Content 113 service consists of two executable software applications: the SC(s) Processor 192 and the Player Application 195. The SC(s) Processor 192 is an executable application which is configured as a Helper Application into the End-User(s) **Web** Browser 191 to handle SC(s) File/MIME Types. This application is launched by the Browser whenever SC(s) are received from the **Electronic**

Digital Content Store(s) 103, the Clearinghouse(s) 105, and the Content Hosting Sitc(s) 1 1 1. It is responsible for performing all required processing of the SC(s) and eventually adding Content 1 13 to the **Digital** Content Library 196 of the End-User(s).

The Player Application 195 is a stand alone executable application which the End-User(s) loads to perform Content 113 in his **Digital** Content Library 196, manage his **Digital** Content Library 196 and create copies of the Content 1 1 3 if permitted. Both the Player Application 195 and SC(s) Processor 192 applications... ...and browsing of Content 113 information, previewing of, for example, song clips, and selecting songs for purchase is all handled via the End-User(s) **Web** Browser 191. **Electronic Digital** Content Store(s) 103 provides the shopping experience in the same way that is offered today by many Content II 3 retailing **web** sites. The difference to the End-User(s) over today's **web** based Content II 3 shopping is that they may now select downloadable Content 113 objects to be added to their shopping cart. If the **Electronic Digital** Content Store(s) 103 has other merchandise available for sale in addition to the downloadable objects, the End-User(s) may have a combination of physical and **electronic** downloadable merchandise in his shopping cart. The Secure **Digital** Content **Electronic** Distribution End-User Device(s) 109 are not involved until after the End-User(s) checks out and submits his final purchase authorization to the **Electronic Digital** Content Store(s) 103. Prior to this point, all interaction is between the **Web** Server for the **Electronic Digital** Content Store(s) 103 and the Browser 191 on the End-User Device(s) 109. This includes preview of sample **Digital** Content clips. **Digital** Content clips are not packaged into SC(s) but instead are integrated into the **web** service of the **Electronic Digital** Content Store(s) 103 as downloadable files or fed from a streaming server. The format of the Content 113 clip is not dictated by the system architecture. In another embodiment, the Player Application 195 could interact directly with the **Electronic Digital** Content Store(s) 103 or Clearinghouse(s) 105 or offline using a promotional CD.

B. Application Installation
The Player Application 195 and the Helper Application 1991 are packaged into a self installing executable program which is available for download from many **web** sites. The Clearinghouse(s) 105 acts as a central location which hosts the master download page at a public **web** site. It contains links to the locations from which the installation package can be downloaded. The installation package is available at all Content Hosting Site(s) I 0 1 1 1 to provide geographic dispersal of the download requests. Each participating **Electronic Digital** Content Store(s) 103 can also make the package available for download from their site or may just provide a link to the master download page at the public **web** site of the Clearinghouse(s) 105.

Any End-User(s) wishing to purchase downloadable Content 113, downloads and install this package. The installation is self... ...package. It unpacks and installs both the Helper Application 198 and the Player Application 195 and also configure the Helper Application 198 to the installed **Web** Browser(s).

As part of the installation, a Public/Private Key 661 pair is created for the End-User Device(s) 109 for use in processing Order and **License** SC(s) 660. A random Symmetric

Key (Secret User Key) is also generated for use in protecting song encryption keys in the **License** Database 197. The Secret User Key (not shown) is protected by breaking the key into multiple parts and storing pieces of the key in multiple...One product this code was introduced is in the IBM ThinkPad 770 laptop computer. Here, the tamper-resistant software was used to protect the DVD **movie** player in the computer. **Digital** Content Provider(s) such as Hollywood studios, concerned about the advent of **digital movies** and the ease at which perfect copies can be made, have insisted that **movies** on DVD disc(s) contain copy protection mechanisms. IBM's tamper-resistant software made it difficult to circumvent these copy protection mechanisms. This is a... ...hackers regarding its true operation. The latter technique is largely ad hoc, but the first two build upon well-known tools in cryptography: encryption and **digital** signatures.

C. Secure Container Processor 192

When the End-User(s) submits the final purchase authorization to the **Electronic Digital** Content Store(s) 103 for the merchandise he has collected in his shopping cart, his **Web** Browser remains active waiting for a response from the **Web** Server. The **Web** Server at the **Electronic Digital** Content Store(s) 103 processes the purchase and performs the financial settlement and then returns a Transaction SC(s) 640 to the End-User Device(s) 109. The SC(s) Processor 192 (Helper Application 198) is launched by the **Web** Browser to process the SC(s) mime type associated with the Transaction SC(s) 640. FIG. 14 is an example of user interface screens of... ...displayed with this information and the End-User(s) is presented with options to schedule the download(s) of the Content 113 (e.g. for **music**, songs or entire albums), step 1402. The End-User(s) can select immediate download or can schedule the download to occur at a later time... ...at install time. This Order SC(s) 650 is sent via HTTP request to the Clearinghouse(s) 105. When the Clearinghouse(s) 105 returns the **License** SC(s) 660, the Helper Application-198 is re-invoked to process the **License** SC(s) 660. The **License** SC(s) 660 is then opened and the URL of the Content Hosting Site(s) 1 1 1 is extracted from the referenced Order SC(s) 650. The **License** SC(s) 660 is then sent to the specified Content Hosting Site 1 1 1, via http request through the Browser, requesting download of the... ...a buffer is filled, it is decrypted using the Key 623 (corresponding to the Public Key 661) of the End-User(s) extracted from the **License** SC(s) 660, which itself is first decrypted using the Private Key.

The decrypted buffer is then passed to the watermarking function.

The watermarking 193 extracts the watermarking instructions ftom the **License** SC(s) 660 and decrypt the instructions using the Private Key of the End-User(s). The watermarking data is then extracted ftom the **License** SC(s) 660 which includes transaction information such as the purchaser's name as registered with the **Electronic** I 0 **Digital** Content Store(s) 103 from which this Content 113 was purchased or derived from the credit card registration information if the **Electronic Digital** Content Store(s) 103 does not provide a registration function.

Also included in the watermark is the purchase date and the Transaction ID 535 assigned by the **Electronic Digital** Content Store(s) 103 to reference the specific records logged

for this transaction. The Store Usage Conditions 519 are also included to be used by...

...encrypt the Content 113 using a random Symmetric Key. Once the download and Decryption and Re-Encryption 194 process is complete, the encryption Key 623 **used** by the **Content** Provider(s) 101 to originally encrypt the Content 113 is now destroyed and the new SEAL key is itself encrypted using the Secret User Key created and hidden at installation time. This new encrypted Seal Key is now stored in the **License** Database 107.

Unlike source performed at the Content Provider(s) 101 and user watermarking performed at the End User Device(s) 109 may need to become an industry standard to be effective. These standards are still evolving. The technology is available to allow control information to be embedded in the **music** and updated a number of times.

Until such time as the copy control standards are more stable, alternative methods of copy control have been provided in the Secure **Digital** Content **Electronic** Distribution System 100 so that it does not rely on the copy control watermark in order to provide **rights** management in the consumer device. Storage and p lay/record usage conditions security is implemented utilizing encrypted DC Library Collections 196 that are tied to...

...Environment. Software hooks are in place to support copy control watermarking when standards have been adopted. Support exists today for watermarking AAC and other encoded **audio** streams at a variety of compression levels but this technology is still somewhat immature at this time to be put to use as a sole... ...in the selection of the original content encryption algorithm. Thus use of widely accepted and proven industry standard algorithms can be used thus further enhancing **Digital** Content Industry acceptance of the Secure **Digital** Content **Electronic** Distribution System 100.

The second purpose of this Decryption and Re-Encryption 194 process is to remove the requirement that the original master encryption Key 623, **used** by the **Content** Provider(s) 1 0 1 to encrypt this Content I 1 3, be stored on every End-User Device(s) 109 which has **licensed** this Content 1 1 3. The encrypted master Key 623, as part of the **License** SC(s) 660, is only cached on the hard disk of the End-User Device(s) 109 for a very short time and is in... ...Encryption 194 phase has completed, greatly lessens the possibility of piracy from hackers.

Once the song has been re-encrypted, it is stored in the **Digital** Content Library 196. All metadata required for use by the Player Application 195, is extracted from the associated Offer SC(s) 641 and also stored in the **Digital** Content Library 196, step 1403. Any parts of the metadata which are encrypted, such as the song lyrics, are decrypted and re-encrypted in the... ...to encrypt the Content II 3 is used for any associated metadata needing to be encrypted.

D. The Player Application 195
1. Overview
The Secure **Digital** Content **Electronic** Distribution Player Application 195 (referred to here as the Player Application 195) is analogous to both a CD, DVD or other **Digital** Content player and to a CD, DVD, or other **digital** content storage management system.

At its simplest, it performs Content 113, such as playing songs or videos. At another level, it provides the End- User(s) a tool for managing his/her **Digital** Content Library 196.

And just as importantly, it provides for editing and playing of collections of content, such as songs, (referred to here as Play... ...195 is assembled from a collection of components that may be individually selected and customized to the requirements of the Content Provider(s) 101 and **Electronic Digital** Content Store(s) 103. A generic version of the player is described, but customization is possible.

Referring now to FIG. 15 there is shown a... ...sets may be selected, based on the requirements of.

the platform (Windows, Unix, or equivalent)
communications protocols (network, cable, etc)
Content Provider(s) 101 or **Electronic Digital** Content Store(s) 103
Hardware (CD, DVD, etc)
Clearinghouse(s) 105 technology and more.

The sections below detail the various component sets. The final section... ...no definitive layout of these components. One such layout is provided in the generic player. Based on requirements from Content Provider(s) 101 and/or **Electronic Digital** Content Store(s) and other requirements, alternate layouts are possible.

This set is grouped into subgroups, starting with the components used to present End-User Display 15 1 0 and handle controls called End-User Controls 1511 used for such low-level functions as **audio** playback , and presentation of metadata. Next, the End-User Display Component 1510 is further divided by special function groupings (Play-list, **Digital** Content Library), and then object-container components used for grouping and placing of those lower-level components.

Within the component listings below, any reference to... ...to a CD or other recordable medium only applies to the case where the Player Application 195 has such functionality enabled.

Also note that the **term** CD in that context is a generic one, that can also represent various other external recording devices, such as MiniDisc or DVD. 1 5 FIG... ...the Content 1 13.

Play/Stop button
Play button
Stop button
Pause button
Skip forward button
Skip backward button
Volume control

Track position control/display
Audio channel volume level display and more.

Controls for the displaying metadata associated with the Content II 3
Cover Picture button
Cover Picture object
Artist Picture... ...include (corresponding screens of an End-User Interface are shown 1601 - 1605).

Play-list of display container
Play-list Management button
Play-list Management window
Digital Content search button
Digital Content search Definition object
Digital Content search Submit button
Digital Content search Results object
Copy Selected Search Result Item To. Play-list button
Play-list object (editable)
Play-list Save button
Play-list Play button
Play-list Pause button
Play-list Restart button
Create CD from Play-list button and more.

Display of **Digital** Content Library 196
Digital content library button
Digital content librarian window
Digital content categories button
Digital content categories object
By-artist button
By-genre button
By4abel button
By-category button
Delete button
Add-to-Play-list button
Copy to CD button
Song List object
Song List display container and more
I 0
Containers and Misc.

Player window container
Audio controls container
Metadata controls container
Metadata display container
Toolbar container object

Sample button
Download button
Purchase button
Record button
Player Name object
Label/Provider/Store...The use of the Content 113 by the Player Applications 195 on End
User Device(s) 109 is logged into a database such as the **License** Database 197.
Thetracking of each use of Content 113 bythe Player Application 195 can be transmitted
to one or more logging sites such as the Clearing House(s) 105 or Content Provider(s)
101 or **Electronic Digital** Content Store(s) 103 or any site designated and coupled to
Transmission Infrastructures 107.

This transmission can be scheduled at predetermined times to upload the... ...example,
when duplicating or copying the Content 113 stored at the End User Device(s) 109, on to
an external device such as DVD Disc, **digital** tape, flash memory, mini Disc or
equivalent read/writeable removable media, the use is updates to the logging site. This
may be a precondition to... ...Content I 1 3 was performed; if the Content II 3 has been
duplicated or copied to an authorized external device such as DVD Disc, **digital** tape or
mini-Disc. In cases where there are multiple distinct users of a single Player Application
195 on the End User 1 5 Device... ...any one time and the results extrapolated. In this
present embodiment, the actual usage can be measures for the users logging back onto a
designated **web** site such as the **Electronic Digital** Content Storc(s) 103 or Content
Provider(s) 101.

4. Decryption 1505, Decompression 1506 and Playback Components 1506
These components use the keys acquired by the Copy/Play Management components to
unlock the **audio** data acquired from the Data Management and Library Access
components, apply the appropriate decompression to prepare it for playback, and use
system **audio** services to play it. In an alternate embodiment, the **audio** data acquired
from the Data Management and Library Access components may be copied to removable
media such as CDS, diskettes, tapes or MiniDisks.

5. Data... ...well as handle requests for information about the stored songs.

6. Inter-application Communication Components 1508
These components are used for coordination between the Secure **Digital** Content
Electronic Distribution Player and other applications (e.g., Browser, helper-app and/or
plug-in, etc) that may invoke the Player Application 195, or that the... ...are required for
any player, but may be replaced by specialized versions depending 1 5 on such things as
form of encryption or scrambling being **used**, types of **audio** compression, access
methods for the Content 1 1 3 library, and more.

Above the Player Object Manager 1501 are Variable Objects 1512, which are mostly
Player Application 195
The following embodiment is for an example where the Player Application 195 running
on End-User Device(s) 109 is an **audio** player where Content 113 is **music**. It should be

understood to those skilled in the art that other types of Content 113 can be supported by the Player Application 195. A typical **audio** enthusiast has a library of CDS holding songs. All of these are available within the Secure **Digital** Content **Electronic** Distribution System 100. The set of songs that have been purchased from **Electronic Digital** Content Store(s) 103 are stored within a **Digital** Content Library 196 on his or her system. The groupings of songs that are analogous to physical CDS are stored as Play-lists. In some cases a Play-list exactly emulates a CD (e.g., all tracks of a commercially available CD has been purchased from an **Electronic Digital** Content Store(s) 103 as an on-line version of the CD and is defined by a Play-list equivalent to that of the CD). But most Play-lists is put together by End-User(s) to group songs they have stored in the **Digital** Content Libraries on their systems. However for the purposes of the ensuing discussions, an example of a custom made **music** CD is **used** when the **term** a Play- list is mentioned.

When the End-User(s) starts the Player Application 195 explicitly, rather than having it start up via invocation from the SC(s) Processor 192 Application, it pre-loads to the last Play-list that was accessed. If no Play-lists exist in the **Digital** Content Library 196, the Play-list editor is started automatically (unless the user has turned off this feature via a preference setting). See The Play... ...End-User Interface 1603).

When the End-User(s) has invoked the Play-list function, these are the available functions.

Open Play-list
I 0 **Digital** Content Librarian is invoked to display a list of stored Play-lists for selection. Also see **Digital** Content Librarian below for more info.

Edit Play-list
Invokes the Play-list Editor (see below), primed with the current Play-list if one has... ...for more info.

Play-list Info
Display information about the Play-list.

Song Info
Display information about the selected song within the Play-list.

Visit **web** site
Load **web** site associated with this Play-list into browser.

Librarian
Open the **Digital** Content Librarian window. Also see **Digital** Content Librarian below for more info.

The Play-list Editor (corresponding screen of an End-User Interface 1603).

When invoking the Play-list editor, these are the End-User(s)' options.

View/Load/Delete Play-lists
Digital Content Librarian is invoked to display a list of stored Play-lists for selection of one to load or delete. Also see **Digital** Content Librarian below for more info.

Save Play-list
Current version of Play-list is saved in the **Digital** Content Library 196.

Delete Song
Currently selected song is deleted from Play-list.

Add Song
Digital Content Librarian is invoked in song-search mode, for selection of song to add to the Play-list. Also see **Digital** Content Librarian below for more info.

Set Song Information
Display and allow changes to information about the selected song within the play-list. This information is stored within the Play-list, and does not alter information about the song stored within the **Digital** Content Library 196. These things can be changed.

Displayed Song Title
I 0 End-User(s) notes about the song
Lead-in delay on playing... ...play once, restart when done, etc)
End-User(s) notes about this Play-list
Librarian (corresponding screen of an End-User Interface 1601).

Open the **Digital** Content Librarian window. Also see **Digital** Content Librarian below for more info.

Song Play
When a song has been prepared for play, either by invoking the Player Application 195 with the song as an argument or by selecting a song for play ftom a Play-list or within the **Digital** Content Librarian, these are the End-User(s)' options: (corresponding screen of an End-User Interface 1601).

Play
Pause
Stop
Skip Backward
Skip Forward
Adjust Volume
Adjust Track Position
View Lyrics
View Credits
View CD Cover

View Artist Picture
View Track Information
View other metadata
Visit **web** site
Play-list
Librarian and more.

I 0
Digital Content Librarian
The **Digital** Content Librarian can be invoked implicitly when selecting songs or Play-lists (see above) or may be opened in its own window for management of...

Claims:

...the usage condition data to create promotional data; and transferring the promotional data. II. The system of claim 1 0 wherein the content data includes **music** data, and the usage condition data 1 5 includes at least one of a time restriction on the playing of the **music** data, a maximum number of copies of the **music** data that can be made and a maximum number of times the **music** data can be played.

12 The system of claim IO,
wherein the content data includes **music** data, andthe metadata includes at least one of a link to a content data host, a description of the content of the **music** data, artwork associated with the **music** data, and a selected portion of the **music** data.
13 An **electronic** content management system for managing content data, associated metadata, and associated
usage condition data, said system comprising:a content provider capable of transmitting associated metadata of content data, and associated usagecondition data of content data; andan **electronic** store capable of receiving the metadata and the usage condition data from the content provider and generating altered promotional data from at least one of...
...encrypting key with a second encrypting key; and transmitting the encrypted first encrypting key.
15 The system of claim 13,
wherein the content data includes **music** data, andthe usage condition data includes at least one of time restrictions on the playing of the **music** data a maximum number of copies of the **music** data that can be made and a maximum number of times the **music** data can be played.
16 The system of claim 13,
wherein the content data includes **music** data, andthe metadata transmitted at least one of the information identifying the content provider, a link to the content host; and at least one of a description of the content of the **music** data, artwork associated with the **music** data, and a selected portion of the **music** data.I 0
17 The system of claim 13 wherein the content provider is capable of transmitting content data, the system further comprising a content host capable of receiving the content data from the content provider.

18 A **digital** content data player for playing **digital** content data, said data player comprising a transmitter for transmitting usage information, the usage information being at least one of the occurance of the playing or copying of the **digital** content data, the number of times the **digital** content data was played or copied, the time the **digital** content data was played or copied, and the identification of a user that plays or copies the **digital** content data.

19 The data player as defined in claim 18, wherein the **digital** content data includes **digital music** data.

20 A system for tracking usage of **digital** content comprising:
a **license** to play or copy **digital** content data;**licensed digital** content data;
andinformation on at least one of the occurrence of playing or copying of the **licensed digital** content data, the number of times the **licensed digital** content data was played or copied, the time the **licensed digital** content data was played or copied and the identification of a user that plays or copies the **licensed digital** content data.
21 The system of claim 20 further comprising prohibiting further playing or copying based on the information.

22 The system in claim 20, wherein the **digital** content data includes **digital music** data.

23 The system of claim 20, wherein the information is transmitted at a predetermined time or at a predetermined interval.

26 A computer readable medium containing program instructions for tracking usage of **digital** content data on
user devices, comprising instructions for:obtaining a **license** to play or copy **digital** content data;accepting the **licensed digital** content; andtransmitting information on at least one of playing of the **digital** content data, copying of the **digital** content data, the time the **digital** content data was played or copied and the identification of a user that plays or copies the **digital** content data.r@ @CONTENT PROVIDER(S) --op. PCM123 @ 121 FILESCONTEN CLF Nit154 160METADATA 126lol 122SECURE CONTAINER PACKER... ...CLRNGH @COE5@5@@130 CLRNGHCONTENT USAGEPROMOTIONS coLCONTENT10029FIG.]A131171 180 1I CONTENT EXTRACTED METADATA,ACQUISITION GRAPHICS, **AUDIO** CLIPS 1@32@@@@ CONTENTOOL 173 DBMETADATA SC OFFER SC133 CLRNGH CLRNGH 1811 eCOMMGPBp C CMNGHUSAG (rLRNGHI DB IC... ...NOTIFI(PROCESSOR INTEFSECURE CONTAINER PACKER TOOLMODULE mocTRANSACTION SCo4TRANSACTION IDCLRNGH IONLOGOFFER SCCLRNGH ACCOUNTOFFER SC RECONCILIATION I**ELECTRONIC DIGITAL**I CONTENT STORE(S) Z'FIG. IB '00107141370RDER SC LICICLRNGH=% CLRNGH105 END-USERDATA184 NOWCUSTOMER 185- ERVICE... ...ILLING LOGSSYSTEMloo 0CLFIG. ICCONTENT HOSTING SITE(S) 148 CONTENT SC I I END USER DEVICE(S)CLRNGHCONTENT191147 **WEBOEM OEM LICENSE** SC

11 BROWSER 196M mm OEM I i192 SECURE DCCLRNGH=%Em m I I CONTAINER LIBRARYPROCESSOR COLLECTION11198HSIVIS I I HELPER1 1193 APPLICATION **LICENSE**CONTENT I I WATER- DI3LIBRARY IVIGIVIT 11 MARKING1194 DECRYPTIONLm I REI ENCRYPTION'mm I140 141 146100FIG. IDSC... ...Im IIz zcRo N, Im mm ImSC PROCESSING SC PROCESSING--------------- TRANSACTION 10,Q)VERIFICATION I........................... Q)m ------ @"ww@ --- N> **LICENSE** L **LICENSE** REQUESTZ AUTHOURIZATIONG) .... ol .... w ....r 4AUDIT/REPORTING co DECRYPTIONc: .... 0----------------- - - - --------------------------- - ...cnm **LICENSE**cn WATERMARK.......................... . ... ---COPY/PLAY CODEUSAGE CONDITONS 4`VALIDATIONSCRAMBLING/STOREco. . . . .0 m DE-SCRAMBLING QVIm zDECOMPRESSIONm cnU) mOM... ...630641 640 621 CONTENT608CLRNGHOFFER SC(S) CPTRANSACTION 7775&IJ(SEE DETAIL) ID 624602 642CONTENT 103 643 604113**ELECTRONIC** SER630--"1 624 **DIGITAL** CONTENT --ad DEVICE(S)621 623 517 STORE(S) -"ORRCLRNGH 650 623 6031 642601 C @& CLRNGH 6TRANSACTIONID 605606624... ...too*806METADATA S7' CONTENT SCCREATION CREATION807813FINAL QUALITYASSURANCE+ 814CONTENT DISPERSEMENTCONTENTPROMOTIONS 156SITECONTENTFEXTRACTED METADATA,CONTENT GRAPHICS, **AUDIO** CLIPS CONTENTPROMOTIONS N`@171 173 180 DBTOOL METADATA SC OFFER CCLRNGH CLRNGH 1 eCOMMERCECLRNGH CLRNGH OFFERUSAGE USAGE DBCOND's... ...TRANSACTION NOTIFIiPROCESSOR INTEFSECURECONTAINERPACKERTOOLMODULE MO[@N@ lle@TRANSACTION SC17TRANSACTION IDCLRNGH TRANSACTIONLOGOFFER SCCLRNGH ACCOUNTOFFER SC RECONCILIATION TOOL**ELECTRONIC** TRANSACTION ID**DIGITAL**CONTENTSTORE(S) OFFE SC103 TRANSACTIONCE5@;ROFFER SC SC191**WEB**BROWSERCLRNGH CLRNGH 192END- USER ORDERSC IDATA SECURE /loooCONTAINER DC105 198 PROCESSOR LIBRACOLLEC'ENDUSR**LICENSE** SC I HELPERAPPLICATION N %cCLEARINGHOUSE (S) 193 DBLWATERCONTENT ENDUSR **LICENSE** SC MARKINGHOSTINGSITE(S) 194tDECRYPTIONRECONTENT SC ENCRYPTIONL1101SELECT ALGORITHM& BIT RATE1102YES HERE A 0PREVIOUSLY CALCU... ...103 11 08RETRIEVE PREVIOUSLY CALCULATED BEGIN ENCODING FOR ARATE FACTOR RSTORED PREDETERMINED PERIODOF TIME & CALCULATE NEW/,oo@ 1104 RATE FACTOR RNEWENCODE **DIGITAL** CONTENT & DISPLAY 1109PROGESS USING RSTOREDENCODE **DIGITAL** CONTENT &1105 DISPLAY PROGRESSUSING RNEWCALCULATE CURRENTRATE FACTOR RCURRENT/,*@ 1106UPDATE RATE FACTOR RNEW = AVG (RSTORED + RCURRENT)1107STORE RNEW FOR THIS ALGORITHM... ...ISMN OR EQUIVALENT)tloo@ 1202INDEX INTO CONTENT PROVIDER'SDATABASE(S) USING IDENTIFIER/ooo@ 1203RETRIEVE ADDITIONALINFORMATION RELATED TO MEDIAtlo@ 1204CREATING **DIGITAL** CONTENTFOR **ELECTRONIC** DISTRIBUTIONFIG* 121301SELECT **MUSIC** TO BE ENCOD1302DETERMINE GENRE OF **MUSIC**SELECTED/@7 1303DETERMINE **AUDIO** COMPRESSIONLEVELS &

AUDIO COMPRESSIONALGORITHMS TO BE USED FOR
ENCODING1304SELECT AUDIO SIGNAL PROCESSINGOPERATIONS &
COMPRESSION SETTINGSFIG* 137120SCHEDULE DOWNLOAD1401USER
STARTS A DOWNLOADDOWNLOAD1402DOWNLOAD
COMPLETESLIBRARY14034 Play C13,;FIG* 141509 1511PLAYER musicWINDOW
D(END-USER END-UllCONTROLS TOOLBAR DISPLCONTAllAUDIO DE
CONTROLS CONTR1512VARIABLE OBJECTS1501PLAYER OBJECT
MANAGER1502 1504DATA COPY/PLAY DECOMPRIMANAGEMENT
MANAGEMENT503 1505LIBRARY ECRYPTIONACCESS/,,@ 1508...

SYSTEMS AND METHODS FOR MATCHING, SELECTING, NARROWCASTING, AND/OR CLASSIFYING BASED ON RIGHTS MANAGEMENT AND/OR OTHER INFORMATION

	Country	Number	Kind	Date
Patent				19

English Abstract:

Rights management information is used at least in part in a matching, narrowcasting, classifying and/or selecting process. A matching and classification utility system comprising a... ...non-limiting examples of which include software objects. The Matching and Classification Utility system may use any pre-existing classification schemes, including at least some **rights** management information and/or other qualitative and/or parameter data indicating and/or defining classes, classification systems, class hierarchies, categroy schemes, class assignments, category assignments, and/or class membership. The Matching and Classification Utility may also use at least some **rights** management information together with any artificial intelligence, expert system, statistical, computational, manual, or any other means to define new classes, class hierarchies, classification systems, category...

Detailed Description:

SYSTEMS AND METHODS FOR MATCHING,
SELECTING, NARROWCASTING9 AND/OR
CLASSIFYING BASED ON **RIGHTS**
MANAGEMENT AND/OR OTHER

INFORMATION
FIELDS OF THE INVENTIONS
The inventions relate to **electronic rights** and transaction
management. More particularly, the inventions relate to automated
1 0 systems, methods and techniques for efficiently matching, selecting,
narrowcasting, categorizing and/or classifying in a distributed
electronic rights and/or other event and/or transaction management
environment. For example, the inventions provide **electronic**
computer based systems, methods and techniques for matching,
1 5 classifying, narrowcasting, and/or selecting **digital** information
describing people and/or other things. This matching, classifying,
narrowcasting, and/or selecting can be based, at least in part, on
elements of **rights** management information and/or one or more other
categories of information -- wherein such information is used for
efficient, trusted event management assuring the execution of one or
more controls related to, including, for example, consequences of
processing such **digital** information describing people and/or other
things. The present inventions also provide systems and methods for
efficiently determining class hierarchies, classification schemes,
categories, and/or... ...and/or the assignment of objects,
persons and/or things to said class hierarchies, classification schemes,
categories, and/or category schemes using at least some **rights**
management information.

BACKGROUND AND SUMMARY OF THE
INVENTIONS
The modem world gives us a tremendous variety and range of
options and choices. Cable and satellite television delivers hundreds
of different television channels each carrying a different program.

The radio dial is crowded with different radio stations offering all
kinds of **music**, news, talk, and anything else one may care to listen
I 0 to. The comer convenience store carries newspapers from around the
country, and a... ...they are often located in too many places. We can waste a lot of
time searching for the things we need or want at the **right** price, with
the **rights** features, and at a particular time.

Sometimes, we never find things that satisfy what we feel we
need or want. This happens when we don...golf tournament or golf players being
broadcast at 7
o'clock on a particular channel. After flipping through other
channels, he might think an action **movie** looks interesting only to
find out after watching it for a while that he isn't really interested in it
after all. A documentary on...way,
businesses save time and money and consumers aren't unproductively
hassled by information, phone calls, junk mail, junk e-mail and the

like. However, **right** now it is extremely difficult to accomplish this
I 0 goal, and so businesses continue to annoy consumers while wasting
their own time, money, and... ...time trying to find what you
are looking for. Modem libraries can be huge, containing tens or
even hundreds of thousands or millions of different **books**,
magazines, newspapers, video tapes, **audio** tapes, disks, and other
publications. Most libraries have an **electronic** or manual card catalog
that classifies and indexes all of those **books** and other materials.

This classification system is useful, but it often has significant
limitations.

For example, normally a card catalog will classify materials
based only... ...school report. The card catalog led to the general subject of baseball
and other sports, but, looking at the catalog, he can't identify any
books that seem to provide the specific information he wants to see,
so he must rely on **books** classified as "histories of sports" or
"histories of baseball." He can spend lots of time looking through the
I 0 **books** on the shelves, going back to the card catalog, and going back
to the shelves before he finds a reference that's reasonably helpful.

He may need to go ask an expert (the librarian) who is familiar with
the **books** the library has on sports and may know where to look for
the information. Even then, the boy may need to flip through many
1 5 different **books** and magazines, and look in many different places
within the library before he finds the information he is looking for.

Finding Products You Want or... ...to help
him identify where he wants to buy the tie. Perhaps he uses a mall
I 0 directory that classifies the different stores in **terms** of what kinds of
merchandise they sell (for example, clothing, **books**, housewares,
etc.). Perhaps he asks at the malls help desk staffed by "experts" who
know what is available in the shopping mall. But even these can with the
available resources.

These Problems Are Worse in the **Digital** World
The **electronic** or **digital** world offers a rapidly growing, vast
array of electronically published products and services. For example,
computer superstores have a dizzying array of different software
products. Furthermore, **music** is now published primarily in **digital**
form on optical disks, and video will soon be published that way too.

And, of particular interest related to certain of the inventions
described by this document, the **Internet** now has millions of home
pages with an overwhelmingly variety and quantity of **digital**
information, and, these millions of home pages, in turn, point or

"link" to millions of other **web** pages as well.

Today, for example, you can use the **Internet** to.

read **electronic** newspapers, **books** and magazines and
see them on your computer screen;
get **music** in **electronic** form and play it using your
computer;
send and receive **electronic** mail all over the world;
download reports and other information compiled by
governments, companies, industries, universities, and
individuals;
watch videos and animations;
play games with... ...some interests in common;
participate in "virtual reality" worlds, games, and/or
experiences;
(offer to) buy, and/or (offer to) sell nearly anything;
and
conduct **electronic** transactions and commerce.

Today on the **Internet** and you can also find nearly anything
and everything you can possibly imagine, although finding exactly
what you really want may be time consuming and frustrating. This is
I 0
because the **Internet** and World Wide **Web** provide perhaps the best
example of an environment that is particularly hard to navigate.

There are an overwhelming number of choices -- too many to easily
relate to or understand -- and many of which are terribly hard to find,
even using the various **Web** searching "engines." The **Internet** is
particularly exciting because it has the potential to provide to nearly
everyone access to nearly every kind of information. Information can
also come from an almost limitless variety of sources. But today, so
much information on the **Internet** is superficial or useless, and too
many choices can be more a curse than a blessing if you don't have
meaningful, easy ways to eliminate all but a relatively few choices.

And the situation will only become much worse as more **Web** sites
appear, and as **digital** information is distributed in "objects" or
"containers" providing enhanced security and privacy but possibly
1 5 more difficult access and identifiability.

As time passes, more and more valuable and desirable
information will be available in **digital** containers. However, unless
tools are developed to solve the problem, there will be no efficient or
satisfying means to sort through the potentially trillions of **digital**

containers available on tens of millions of **Web** pages, to find
containers satisfying a search or fulfilling an information need.

Furthermore, existing information searching mechanisms typically
provide no way to readily perform a search that matches against
underlying commercial requirements of providers and users.

It Will Be Difficult to Find **Rights** Management
Scenarios Matching ...redistribute per copy in quantities of several
thousand -- this low cost being particularly important since you will
have numerous other costs per issue for acquiring **rights** to other
1 5 useful **digital** information products which you reuse and, for example,
enhance in preparing a particular issue. You therefore wish to search
and match against **rights** management rules associated with such
products -- non-limiting examples of which include.

cost ceilings,
redistribution **rights** (e.g., limits on the quantity that may
be redistributed),
modification **rights**,
class related usage **rights**,
category related usage **rights**,
sovereignty based **licensing** and taxation fees,
import and export regulations, and
reporting and/or privacy **rights** (you don't want to report
back to the product provider the actual identity of your
end users and/or customers.

If you can't... ...settling on the first adequate product that you review).

Computers Don't Necessarily Make It Easier to Find
Things
Anyone who has ever used the **Internet** or the World Wide **Web**
knows that networks, computers and electronics, when used together,
1 5 do not necessarily make the overall task of finding information easier.

In fact, computers can make the process seem much worse. Most
Internet users will probably agree that trying to find things you are
interested on the **Internet** can be a huge time drain. And the results
can be very unsatisfactory. The rapid growth rate of information
available on the **Web** is continually making this process of finding
desired information even harder. You can spend many hours looking
for information on a subject that interests you... ...With the advent of the technology
advances
developed by InterTrust Technologies Corp. and others, publishers
will find it far more appealing to make their valuable **digital**

information assets available on-line and to allow extractions and modifications of copyrighted materials that will vastly expand the total number of information objects. This will enormously worsen the problem, as the availability of valuable information products greatly expands.

It Is Usually Hard to Find Things On the **Internet**
There are many reasons why it is difficult to find what you want on the Internet. One key reason is that, unlike a public library, for example, there is no universal system to classify or organize **electronic** information to provide information for matching with what's important to the person who is searching. Unlike a library, it is difficult on the **Internet** to efficiently browse over many items since the number of possible choices may be much larger than the number of **books** on a library shelves and since **electronic** classification systems typically do not provide much in the way of physical cues.

For example, when browsing library shelves, the size of a **book**, the number of pictures in the **book**, or pictures on magazine covers may also help you find what you are interested in. Such physical cue information may be key to identifying desired selections from library resources. Unfortunately, most **digital** experiences typically do not provide such cues without actually loading and viewing the work in **digital** form.

Thus, another reason why the **electronic** or **digital** world can make it even harder to find information than ever before has to do with the physical format of the information. The **digital** information may provide few or no outward cues or other physical characteristics that could help you to even find out what it is - let alone determine whether or not you are interested in it, unless such cues are provided through special purpose informational (for example, graphical) displays. On the **Internet**, everyone can be an **electronic** publisher, and everyone can organize their offerings differently -- using visual I 0 cues of their own distinctive design (e.g., location on a **web** page, organization by their own system for guiding choices). As one example, one publisher might use a special purpose graphical representation such as the video kiosk to support an **electronic** video store. Other publishers may use different graphical representations 5 altogether.

Historically, there has been no particular need for consistent selection standards in conventional, non-**electronic** store based businesses. Indeed, it is often the unique display and choice selection support for customers' decision processes that make the difference between a successful store and a failure. But in the **electronic**

display context and/or customized information guidance resource
(catalog **book**, location of goods by size, etc.) seriously undermines
the ability of **digital** information consumers to identify their most
desirable choices.

Adding to this absence of conventional cues, the enormity of
available choices made available in cyberspace means that the **digital**
information revolution, in order to be practical, must provide
profoundly more powerful tools to filter potentially desirable
opportunities from the over abundance of choices. In the **right** "store" and using the
overall arrays of available information
to identify one's selection. However, as information in **digital** and
electronic form becomes more and more important, the problem of
relating to the vast stores of information will become a nightmare.

For example, picture yourself in... ...between a house brand
and a specific name brand, between low fat and regular foods, and
between family size and small size containers.

On the **Internet**, a **digital** "store" is likely to be many stores with
vast resources integrating products from many parties. If you were
limited to conventional classification and matching mechanisms, you While information
written on the "outside" of a **digital** package
may be useful, you simply don't have the time to read all the
packages, and anyway, each packager may use different words to... ...you could limit the number
of choices you were evaluating.

There is a Need For Efficient and Effective Selection
Based, at Least in Part, on **Rights** Management
Information
Unlike a real store where all breakfast cereals are shelved
together and all soft drinks are in the same aisle, there may be no
single, universal way to display the organization of all of the
information in a "**digital** store" since, by its nature, **digital** information
frequently has many implications and associated rules. For example,
there now exist highly developed **rights** management systems such as
I 0 described in U.S. Patent application Serial No. 08/388,107 of Ginter
et al., filed 13 February 1995, for "Systems And Methods For Secure
Transaction Management And **Electronic Rights** Protection (hereafter
"Ginter et al") - the entire disclosure (including the drawings) of
which is expressly incorporated into this application as if expressly
5 set forth herein. Many rules associated with any given piece of **digital**
information may, combinatorially, given rise to many, very different,

commercial contexts that will influence the use decisions of different potential users in many different ways (e.g., cost, auditing, re-use, redistribution, regulatory requirements, etc.).

No readily available systems developed for the **digital** information arena provide similarly satisfying means that describe the many commercial rules and parameters found in individual custom catalogs, merchandise displays, product specifications, and **license** agreements. Further, no readily available mechanisms allow 11surfing" across vast choice opportunities where **electronic** matching can single out those few preferred items.

As one example, picking an appropriate image may involve any or all of the following.

0 price,
0 republishing (redistribution) **rights**,
0 **rights** to extract portions,
0 certified usable in certain sovereignties (e.g., pornographic content not allowed in Saudi Arabia),
I 0 0 size,
0 format, etc... ...based on such criteria.

By their nature, and using the present inventions in combination with, amongst other things, "Ginter et al". the packages in a **digital** store may be "virtual" in nature -- that is, they may be all mixed up to create many, differing products that can be displayed to a prospective customer organized in many different ways. This display may be a "narrowcasting" to a customer based upon his matching priorities, available **digital** information resources (e.g., repository, property, etc.) and associated, available classification information. In the absence of an effective classification and matching system designed to handle such information, **digital** information of a particular kind might be just about anywhere in the store, and very difficult to find since the organization of the stores **digital** information 1 0 resources have not been "dynamically" shaped to the matching interests of the potential customer.

These Inventions Solve These Problems
The present inventions... ...find interesting or important things, things that you enjoy, things that optimize your business efficiency, and things that help you I 0 make the best **digital** products or services you can -- even if you didn't know precisely what or how to look for what you may need. It can also...Reports may be more authoritative on certain topics than more casual reviews published, for example, in the local weekly newspapers.

As another example, consider a **book** that rates restaurants
according several factors, including, for example, quality, price, type
of food, atmosphere, and location. In some locations there may be
many guides... ...priced Cantonese and/or Hunan Chinese
food located in Boston or Atlanta - while weighting the results of the
search in favor of reviews from travel **books** rather than from the local
newspapers. As this example indicates, the searching may be
according to class of authoritative source (and/or classes sources
considered... ...metaclasses."
The Present Inventions Can Make Choices Easier
One simple way to look at some examples of the present
inventions is as a highly sensitive **electronic** "matchmaker" that
matches people or organizations with their best choices, or even
selects choices automatically. The present inventions can match
people and/or organizations with... ...to the specific match circumstances such as the type and/or
purpose of a given match activity.

Figure 5 shows a simplified example of an **electronic**
1 5 matchmaker that can match up two people with like interests. Sarah
loves hiking, country and western **music**, gardening, **movies** and
jogging. Mark loves **movies**, hiking, fast cars, country and western
music, and baseball. The **electronic** matchmaker can look at the
interests, personalities and/or other characteristics of these two people and determine that
they are compatible and should be together... ...may be automatically managed within
1 5 a protected processing environment through the use of controls
contributed by a governmental authority).

Figure 5A shows an **electronic** matchmaker that matches an
electronic publisher with mystery stories for his quarterly **electronic**
mystery anthology, where the matching is based on price,
redistribution **rights**, editing **rights**, attribution requirements
(attributing authorship to the author), third party rating of the writers
quality, length of story, and/or the topical focus of the story (for
example). Here, rule managed business requirements of publisher
and writers are matched allowing for great efficiency in matching,
coordination of interests, and automation of **electronic** business
processes and value chain activities.

The convenience of the "**electronic** matchmaker" provided in
accordance with the present inventions extends to commerce in
physical goods as well -- as illustrated in Figure 5b. In this non
limiting example, the **electronic** matchmaker is communicating to the
consumer via the **Internet** and World Wide **Web**. The matchmaker
has found the lowest quoted price for a Jeep sports utility model

given, in this one example, a multitude of factors including.

I... ...Association, and being a graduate
of Stanford University).

Membership in these associations and alumni status may be conveyed
or indicated by possession of a special **electronic** document called a
"**digital** certificate," "membership card," and/or other **digital**
credential that warrants or attests to some fact or facts.

Thus, the **electronic**' matchmaker provided in accordance with
these inventions can also match people with things. Figure 6 shows
two people, Harry and Tim. Harry loves sports most... ...going on in the business world.

The business world is most important to Tim, but he likes to keep up
with the baseball scores. The **electronic** matchmaker in accordance
with these inventions can learn about what Harry and Tim each like,
and can provide information to a publisher so the publisher... ...over business
1 5 information. But information that Harry and Tim respectively want to
maintain as authentic or secret can be managed as such.

The **electronic** matchmaker can also match things with other
things. Figure 7 shows how the **electronic** matchmaker can help a
student put together a school project about big cats. The **electronic**
matchmaker can help the student locate and select articles and other
material about various kinds of big cats. The **electronic** matchmaker
can, for example, determine that different articles about tigers, lions
and cheetahs are all about big cats - but that articles about elephants
and giraffes are not about big cats. If there is a charge for certain
items, the **electronic** matchmaker can find only those items that the
student can afford, and can make sure the student has the **right** to print
pictures of the big cats. The **electronic** matchmaker can help the
student to collect this information together so the student can make a
colorful poster about big cats.

The **electronic** matchmaker can match up all sorts of different
kinds of things. Figure 8 shows the **electronic** matchmaker looking at
three different objects. The matchmaker can determine that even
though objects A and C are not identical, they are sufficiently similar
that they should be grouped together for a certain purpose. The
I 0 **electronic** matchmaker can determine that for this purpose, object B is
too different and should not be grouped with objects A and C. For a
different purpose, the **electronic** matchmaker may determine that
objects A, B and C ought to be grouped together.

The Present Inventions Can Make Use of **Rights**

1 5 Management Information
How does the **electronic** matchmaker find out the information it
needs to match or classify people and things? In accordance with a
feature provided by these inventions, the **electronic** matchmaker gets
information about people and things by using automated,
computerized processes. Those processes can use a special kind of
information sometimes known as **rights** management information.

Rights management information may include **electronic** rules and/or
their consequences. The **electronic** matchmaker can also use
information other than **rights** management information.

An example of **rights** management information includes certain
records about what a computer does and how it does it. In one simple
example, records may give permission to read... ...pay a nickel to purchase the
article and that the nickel may be paid using a budget provided by a
credit card company or with **electronic** cash. A customer might, for
example, seek only news articles from providers that take **electronic**
cash and/or process information with a certain information
clearinghouse as described in U.S. Patent application Serial No.

I 0 08/699,712 to Shear et al., filed 12 August 1996, for "Trusted
Infrastructure Support Systems, Methods And Techniques For Secure
Electronic Commerce **Electronic** Transactions And **Rights**
Management" (hereafter "Shear et al") - the entire disclosure
(including the drawings) of which is expressly incorporated into this
1 5 application as if expressly set forth herein.

The Present Inventions Can Maintain Privacy
Figure 9 shows one way in which the **electronic** matchmaker
can get information about a person. In this example, the **electronic**
matchmaker asks Jill to fill out a computer questionnaire about what
she likes. The questionnaire can also ask Jill what information she
wishes to be... ...ensure integrity and secrecy, as appropriate.

For example, the questionnaire may ask Jill whether she likes
baseball and whether she is interested in volcanoes. The **electronic**
matchmaker can also ask Jill if it is okay to look at records her
computer maintains about what she has used her computer for in... ...Figure IO, Jill may
have used her computer last
week to look at information about baseball, volcanoes and Jeeps.

5 With Jill's permission, the **electronic** matchmaker can employ a
protected processing environment 154 (schematically shown here as a
tamper-resistant "chip" within the computer - but it can be hardware
based... ...history records and use them to help match Jill

up with other kinds of things she is or may be interested in. For
example, the **electronic** matchmaker can let an **electronic** publisher or
other provider or information gatherer (e.g., market survey conductor,
etc.) know that Jill is interested in team sports, geology and sports
utility vehicles with or without more revealing detail -- as managed
by Jill's choices and/or **rights** management rules and controls
executing in her computer's protected processing environment 154.

The provider can send information to Jill - either automatically or at
Jill's request - about other, related things that Jill may be interested
in.

Figure I I shows an example of how **rights** management and
other information Jill's computer maintains about her past usage can
be useful in matching Jill up with things she may need or... ...less that $1 0 per
item, averages $40 per month in such expenses, and almost never
buys new programs for her computer.

1 5 The **electronic** matchmaker can, with and subject to Jill's
permission, look at and analyze this information. As one example,
the **electronic** matchmaker can analyze relevant rules and controls
provided by third parties who have **rights** in such information -
where such rules are controlled, for example, by Jill's computer's
protected processing environment 154. It can also look at and
analyze Jill's response to computer questionnaires indicating that she
likes baseball and football. The **electronic** matchmaker can, based on
all of this information, automatically select and obtain videos and/or
other publications for Jill about team sports and that cost... ...so that Jill can
preview and select those in which she may have a particular interest
and desire to acquire.

Figure 12 shows that the **electronic** matchmaker can take into
account computer history records for lots of different people. The
electronic matchmaker can work with other **rights** management
related computer systems such as "usage clearinghouses" (non
limiting examples of which are described in each of "Ginter et al" and
"Shear et al") to efficiently collect **rights** management related
I 0 information. The ability to collect history records from many
different people can be very useful. For example, this can allow the
electronic matchmaker to distinguish between things that are very
popular and things that are not so popular.

The present inventions provide great increases in efficiency and... ...resources
particularly appropriate for certain business activities. You can
delegate certain complex tasks to a computer, freeing you to be more
productive and satisfied with **electronic** activities. These automated

processes can be "smart" without being intrusive. For example, they
can learn about your behavior, ...interests and
possible resources are truly best matched.

The present inventions handle many kinds of important issues
and addresses the widest range of information and **rights** and
I 0 automation possibilities. For example, the present inventions are
capable of handling (but are not limited to).

consumer information;
computer information;
business information;
9 entertainment information;
other content information;
information about physical products;
all other kinds of information.

It can reflect and employ all kinds of **rights** to optimize
matching processes, including.

content **rights**;
privacy **rights**;
governmental and societal **rights**;
provider **rights**;
distributor **rights**;
consumer **rights**;
workf[ow **rights**;
other value chain participant **rights**;
e work flow **rights**;
business and personal **rights** and processes of all
kinds.

It can employ all kinds of parameter information, including.

* budget,
* pricing
9 redistribution
* location (of party, item, etc.)
9 privacy... ...of a specific item) can be used in
matching based upon price per unit and/ or total price for a volume
purchase, price for renting, **right** to redistribute, cost for redistributing items, etc.

Privacy can be used for establishing matching contingent upon
usage reporting requirements for viewing, printing, extracting,
dedistributing, listening quality, specific
redistribution **rights**, etc.,

0 creator (e.g., a publisher or manufacturer), distributor,
societal, user, and other participant interests information,
0 0 information generated by automated profiling of... ...intelligence tools for
profiling creation and/or analysis, matching, and/or
negotiation.

The present inventions thus provide for optimal user, provider,
and societal use of **electronic** cyberspace resources (for example,
digital information objects available across the **Internet**, sent by direct
broadcast satellite, transmitted over a cable TV system, and/or
distributed on optical disk).

Of particular importance is the notion of classes... ...typical library subject
and/or author and/or catalog and/or keyword search
and retrieval information systems;
any commercial requirements, associated with the use
of **electronic** information (and/or to products,
I 0 including non-**electronic** products, and/or to any
service), including information embodied in
encrypted rules (controls and/or parameter data)
governing **rights** in **electronic** value chain and
electronic interaction contexts, and further including
1 5 information guaranteed for integrity;
any information descriptive of an available resource
(which may include any information, product, and/or
service, whether available in **electronic** and/or
physical forms) such as: the quality of a **digital**
product as evaluated and ranked and/or otherwise
specified by one or more third parties and/or
independent third parties (e.g., Consumer Reports, a... ...for example, information on how
to
create a nuclear bomb to a confidential government
auditing agency (this allowing free access to
information while protecting societal **rights**);
any information descriptive of a user and/or
department and/or organization and/or class of users
and/or departments and/or organizations (including,
for...provision of classes of
information, entertainment, and/or services to classes
of individuals and/or entities that have (and/or may
I 0 obtain) the **right**(s) to such information and are likely
to find identified information interesting, useful,
and/or entertaining.

The present inventions also provide systems and
methods for... ...and/or the assignment of objects, persons

and/or things to said class hierarchies, classification
schemes, categories, and/or category schemes using at
least some **rights** management information.

e Helps systems, groups, and/or individuals classify,
locate, and/or obtain specific information and/or
classes of information made available through so... ...using, among other things, subject-based addressing
and/or messaging-based protocol layers.

Provides fundamentally important commercial and
societal rules based filtering to identify desired
electronic information and/or **electronic** information
containers through the use of classification structures,
profiling technology, and matching mechanisms that
harness the vast information opportunities in
cyberspace by matching the information... ...against commercial and/or societal rules related
to the use of available information resources,
I 0 including, for example, commercial and/or societal
consequences of **digital** information use imposed as
provider requirements and specified through the use
of, and enforced by the use of, a trusted **rights**
management system such as described in "Ginter et
1 5 al'
Enables content creators and/or distributors to
efficiently "stock the shelves" of retail **electronic**
content outlets and similar merchanisers (both
electronic and hard goods) with products and/or
services most likely to be purchased and/or used by
the customers of such merchanisers. This includes
both barter matching and
negotiated barter and other kinds of matching.

Helps potential customers find those members (e.g.,
objects such as **digital** information containers) of any
one or more classes of content most useful,
entertaining, and/or interesting to them.

* Facilitates organizations securely and efficiently
acquiring and... ...able to
I 0 authorize certain classes of employees to use
specified classes of internal and/or external content.

Efficiently supporting matching between users and
digital information where participants in a chain of

handling and control have specified rules and usage
1 5 consequences for such **digital** information that may
depend on class membership, for example, on
class(es) of content and/or class(es) of value chain
participants and/or classes of **electronic** events,
wherein such participants include, for example, users
and/or participants- contributing rules and
consequences.

Enables first individuals and/or organzations to locate
efficiently other...and/or usage
consequences dependent on membership in one or
more classes where class membership may be
1 5 indicated by posession of a special **digital** document
called a "certificate."
Enables rightsholders to employ rules and/or usage
consequences at least partially dependent on roles and
responsibilities within an organization, where those
roles and responsibilities may be indicated by
posession of a **digital** certificate, **digital** membeship
card, and/or other **digital** credential.

Facilitates more efficient automation of
manufacturing and other workflow processes by, for
example, matching certain manufacturing steps and/or
processes with performance parameter data associated
with available classes of equipment capable of
performing those steps and/or processes.

Makes easier the administration and enforcement of
government and/or societal **rights** by, for example,
providing matching means for automatically applying
certain classes of tax rules to appropriate classes of
sales and other transactions.

Enables altering the... ...and usage consequences and the
presentation of information to vary according to the
difficulty of the information, including, for example,
adjusting the difficulty of an **electronic** game so that it
is neither too frustratingly difficult nor too easy to
use.

Enables a user to efficiently locate content in one or
more...based upon
matching the part's membership in one or more
1 5 classes identified by trusted, commercial controls

employed through the use of a **rights** management
system.

Enables users to search for, locate, and use only those
parts of a document that belong to one or more
specified classes, including... ...to
certain classes of events.

The above capabilities, and others described in this application,
are often ideally managed by distributed commerce nodes of a
distributed, **rights** management environment embedded in or
otherwise connected to the operating system clients of a distributed
computing environment such as described in "Ginter et al" and... ...Of Many Kinds Of
Information And/Or Data
As discussed above, these inventions provide, among other
things, matching, classification, narrowcasting, and/or selection based
on **rights** management and other information. In particular preferred
examples, these matching, classification, narrowcasting, and/or
selection processes and/or techniques may be based at least in part on
rights management information. The **rights** management information
may be an input to the process, it may be an output from the process,
and/or the process can be controlled at least in part by **rights**
management information. Information in addition to, or other than,
rights management information may also be an input, an output,
and/or a basis for controlling, the process and/or techniques.

Rights management information may be directly or indirectly
inputted to the matching, classification and/or selection process. For
I 0 example, **rights** management controls, rules and/or their consequences
may be an input. Examples of such controls and/or rules include
object registration related control set data...including, some, all
or none of the information set forth above.

The processes, techniques and/or systems provided in
accordance with these inventions may output **rights** management
1 5 related information such as, for example.

one or more control sets;
various rules and/or consequences;
information used by control sets;
certificates;
9 other **rights** management information.

In accordance with various preferred embodiments provided by
these inventions, information other than **rights** management
information may also be used, at least in part, as an input, output

and/or to control the matching, classification, narrowcasting, and/or
selection... ...preferred
examples can associate any kind of information, object or thing with
any other kind of information, object or thing.

Different Associations Between Classes and **Rights**
The processes, systems and/or techniques provided in
accordance with these inventions can provide and/or take into account
many different kinds of associations between classes and **rights**. For
example, they can look at what **rights** are available to a user,
computer, data structure or any other object. They can also look to
rights selected by an object (for example, the subset of **rights** a user
has chosen or otherwise identified). Alternatively or in addition, they
can look to **rights** that have been exercised by a user or in conjunction
with an object or other thing, and they can look to the consequences
of exercising such a **right**(s).

Embodiments in Accordance With the Present
Inventions Can Be Used to Define Classes Based on Uni
I 0 Dimensional and/or Multi-Dimensional Attributes...upon and can work with the
arrangements
disclosed in "Ginter et al"; "Shear et al"; and other technology related
1 5 to transaction and/or **rights** management, security, privacy and/or
electronic commerce.

For example, the present inventions can make particular use of
the security, efficiency, privacy, and other features and advantages
provided by the Virtual Distribution... ...specific examples, the present
inventions can be used in combination with (and/or make use of) any
or all of the following broad array of **electronic** commerce
technologies that enable secure, distributed, peer-to-peer **electronic**
rights, event, and/or transaction management capabilities.

a WDE" ("virtual distribution environment") providing,
for example, a family of technologies by which
applications can be created, modified, and/or reused;
a standardized control and container environment which
1 0 facilitates interoperability of **electronic** appliances and
efficient creation of **electronic** commerce applications
and models;
a programmable, secure **electronic** transaction
management foundation having reusable and extensible
1 5 executable components;
seamless integration into host operating environments of
electronic appliances or direct employment of such
technologies in **electronic** commerce applications;

cyberspace **digital** content **rights** and transaction
management control systems that may operate in whole
or in part over Internets, Intranets, optical media and/or
over other **digital** communications media;
support of an **electronic** "world" within which most
forms of **electronic** transaction such as content usage,
distribution, auditing, reporting, and payment activities
can be managed;
0 Transaction Operating Systems (operating systems that
have integrated secure, distributed, and programmable
transaction and/or event management capabilities);
0 **Rights** Operating Systems (operating systems that have
integrated, distributed, and programmable **rights**
management capabilities);
0 secure content container management;
0 clearinghouse functions related to content usage;
0 overall **electronic** commerce architectures that provide
electronic commerce automation through the use of
secure, distributed **digital** events management;
0 the general enablement of traditional commerce behavior
1 5 in the **digital** commerce world;
enhanced inherent, distributed efficiencies of
conventional commerce practices with powerful, reliable
electronic security, and with the programmability and
electronic automation efficiencies made possible by
modem computing;
trusted operation of a freely configurable, highly
efficient, general purpose **digital** marketplace in which
parties "come together" to establish commercial
relationships;
support of "real" commerce in an **electronic** form (that is,
the progressive creation of commercial relationships that
form, over time, a network of interrelated agreements
representing a value chain business model);
enabling... ...negotiation between) securely
created and independently submitted sets of content
and/or appliance control information;
0 interconnection of appliances providing a foundation for
much greater **electronic** interaction and the evolution of
electronic commerce;
0 a variety of capabilities for implementing an **electronic**
1 5 commerce environment;
0 a neutral, general purpose platform for commerce;
0 an architecture that avoids reflecting specific distribution
biases, administrative and control perspectives, and
content types;

0 a broad-spectrum, fundamentally configurable and portable, **electronic** transaction control, distributing, usage, auditing, reporting, and payment operating environment;

systems and methods that uniquely enable **electronic** commerce participants to protect their interests during the sequence of activities comprising an **electronic** commerce model;

ability of commerce participants to assure protection by specifying rules and controls that monitor and enforce their interests during the processing of remote commerce events;

permitting commerce participants to efficiently
I 0 participate in, and manage, the distributed **electronic** activities of a **digital** value chain;

allowing commerce model participants to, for example, securely and cooperatively govern and automate the distributed **electronic** activities comprising their
1 5 collective **electronic** business models;

allowing commerce model participants to securely contribute **electronic** rules and controls that represent their "**electronic**" interests;

rules and controls that extend a "Virtual PresenceTMII through which the commerce participants govern remote value chain activities according to their respective, mutually agreed to **rights**;

a Virtual Presence taking the form of participant specified **electronic** conditions (rules and controls) that must be satisfied before an **electronic** event may occur;

rules and controls that enforce the party's **rights** during "downstream" **electronic** commerce activities;

control information delivered by, and/or otherwise available for use with, the VDE content containers constituting one or more "proposed" **electronic** agreements which manage the use and/or consequences
I 0 of the use of such content and which can enact the **terms** and conditions of agreements involving multiple parties and their various **rights** and obligations;

rules and controls from multiple parties forming aggregate control sets ("Cooperative Virtual
5 PresenceTMII) that ensure that **electronic** commerce activities will be consistent with the agreements amongst value chain participants;

control sets defining the conditions which govern interaction with protected **digital** content (disseminated **digital** content, appliance control information, etc.);

conditions used to control not only **digital** information use itself, but also the consequences of such use to protect the individual interests of commerce participants and form cooperative, efficient, and flexible **electronic** commerce business models;

true, efficient **electronic** cooperative governance of value chain activities;

empowering each commerce model participant to securely deliver, and persistently maintain control over, the rules and controls they contributed specifying constraints on, and consequences of, **electronic** conduct;

extending Cooperative Virtual Presence over time and I 0 involving the execution of controls, and the use of content, at physically dispersed locations, such as **Internet** user sites;

a chain of handling and control in which dispersed locations are bound together through the use of secure I 5 communication techniques and unique, secure **digital** container technology;

ability to preserve the **rights** of parties through a series of transactions which may occur at different times and different locations;

extending the ability of **electronic** content providers to control the use of proprietary information;

allowing content providers to limit use to authorized activities and amounts;

allowing participants (e.g., actors... ...a business model to have the ability to embody their range of agreements and requirements, including use limitations, into an "extended" agreement comprising an overall **electronic** business model;

representing such an extended agreement by **electronic** content control information which can automatically enforce agreed upon **rights** and obligations;

a competitive, general purpose **electronic** commerce architecture supporting the distributed, secure "unmanned" **electronic** interaction;

distributing such capabilities across networks and involving the sequence (or **web**) of distributed activities underlying **electronic** value chains;

cooperative **electronic** governance of distributed **electronic** commerce processes that optimizes **electronic** commerce value propositions;

the capability of electronically, remotely representing the interests of commerce participants to support efficient, flexible, commerce model automation;

enabling rules and controls that are independently
contributed by multiple parties to securely merge
together and form the collective rules and controls sets
that reflect the **electronic** commerce agreements between
parties;
using rules and controls sets to collectively,
automatically, govern remote **electronic** conduct;
securely managing the integration of control information
provided by two or more parties;
I 0 constructing **electronic** agreements between VDE
participants that represents a "negotiation" between the
control requirements of two or more parties and enacts
the **terms** and conditions of a resulting agreement;
ensuring and/or enforcing the **rights** of each party to an
1 5 **electronic** agreement regarding a wide range of
electronic activities related to **electronic** information
and/or appliance usage;
the ability to broadly support **electronic** commerce by
securely managing independently delivered VDE
component objects containing control information
(normally in the form of method, data, or load module
VDE objects);
using... ...listed by the derived control information as
required are available and perform their required
function;
I 0 use of independently delivered control components to
allow **electronic** commerce participants to freely stipulate
their business requirements and trade offs;
allowing **electronic** commerce, through the various
control requirements stipulated by VDE participants, to
1 5 evolve into forms of business which are the most
efficient, competitive and useful -- much as with
traditional, non-**electronic** commerce;
providing commerce participants with the ability to
freely fashion the chains of handling and control
pathways that protect data and processes and the freedom
to shape the models within which their Virtual Presence
operates -- allowing commerce participants to optimally
formulate their **electronic** commerce value propositions;
VDEs configured to support the various underlying
agreements between parties that define important
electronic commerce pathways of handling for **electronic**
content, content and/or appliance control information,
content and/or appliance usage information and payment
and/or credit;
allowing content creators and other providers to... ...rules

and controls previously set in a value chain, to freely
fashion control models implementing their Virtual
1 5 Presence by using GUI templates or **rights** programming
languages employing commerce/**rights** management
components;

component based control methods that allow the present
inventions to efficiently operate as a highly configurable
content control system;

content control models that... ...and/or methods, and/or associated data);

control information for Virtual Presence employed in
protected processing environment nodes located at user
sites to ensure that **digital** events are governed in
accordance with the collective **rights** of commerce model
participants;

I 0 **digital** events that launch or require other **digital** events;

digital events that may include, for example, content use
consequences such as collection of audit information,
secure communication of such information, payment for
content use, or... ...the secure
environment of a distributed system of nodes;

the association of Virtual Presence rules and controls
with protected information enclosed within one or more
electronic content containers to achieve a high order of
configurability for Virtual Presence chains of handling
and control;

distribution using VDE that may package both the
electronic content and control information into the same
VDE container, and/or may involve the delivery to an
end-user site of different pieces of the...system to one
or more remote VDE secure sub-systems and/or VDE
compatible, certified secure remote locations;

use of delivery means that may include **electronic** data
storage means such as optical disks for delivering one
portion of said information and broadcasting and/or
telecommunicating means for other portions of said... ...of customers;

allowing content provider modification over time of rules
I 0 and controls to reflect sales, new pricing, special
discounts, etc. - while limiting this **right** by rules and
controls provided by other parties having more senior
rights;

employing secure object container technology to
1 5 efficiently implement Virtual Presence chains of
handling and control;

use of software container technology to significantly
facilitate the organized dissemination of **digital** content,
including the specialized form of **digital** content

constituting **rights** control information;

employing object software technology and using object technology to form containers for delivery of at least in part encrypted or otherwise secured information;

using containers that contain **electronic** content products or other **electronic** information and some or all of their associated permissions (control) information;

0 distributing container objects along pathways involving content providers and/or content users;

securely moving containers between nodes of a VDE arrangement, which nodes operate VDE foundation software and execute control methods to enact **electronic** information usage control and/or administration models;

I 0 employing delivered containers both for distributing VDE control instructions (information) and/or to encapsulate and electronically distribute content which has been at least partially secured;

supporting the essential needs of **electronic** commerce 1 5 value propositions by uniting fundamental configurability with secure Virtual Presence;

virtual presence across virtual networks in accordance with the underlying agreement amongst commerce model participants to allow each participant to enjoy secure, reliable **electronic** automation of commerce models;

allowing each **rights** holder's Virtual Presence at a remote site to possess the sole authority to administer or delegate the participant's **electronic rights**;

0 capabilities that contribute to establishing an environment of trusted cooperative governance;

0 practical enhancements relating to the establishment of secure event management and the maintenance of secure audit, encryption, budget, and other relevant information;

0 control structures for an overall, distributed, secure **rights**/event administration environment;

0 processes for interaction between independently delivered rules and controls, including **electronic** I 0 negotiation;

0 creating distributed **rights** operating systems;

0 integrating control processes into host operating environments;

0 secure semiconductors to support protected processing 1 5 environments;

0 a secure, programmable, **digital** event management component architecture in which components are fully assembleable and reusable;

0 differing assemblages of components formed to reflect

an exhaustive array of commerce model functional
capabilities, overall model implementations, and ad hoc
event management scenarios;

0 support for the full range of **digital** content types,
delivery modes, and reporting and other administrative
activities;

0 traveling objects;

9 smart agents;

0 "atomic" load module operation to support "sparse
space," cost-effective, secure processing semiconductors;

0 smart card and other traveling client nodes;

0 creating **rights** management software container

I 0 technologies, including extraction, embedding, and other
secure container content management processes;

0 Chain of Handling and Control generation of secure
objects (containers) and associated control information;

0 audit reconciliation and usage pattern evaluation

1 5 processes;

0 specialized cryptographic implementations;

0 use of a specialized **electronic rights** and commerce
language, unique applications for fingerprinting and/or
watermarking technologies, secure control structures, the
formulation of new types of metering technologies,
reciprocal event management (employing dispersed user
sites) for automating **web**-like commerce models, and
many other designs and capabilities;

mechanisms to persistently maintain trusted content
usage and reporting control information through both a
sufficiently secure chain of handling of content and
content control information and through various forms of
usage of **electronic** information;

rights managernemt technology supporting persistent,
distributed controls;

means enabling continuing Virtual Presence through
Chains of Handling and Control;

persistency of control as a unique and fundamentally... ...reliable enforcement of
agreements between parties;

Persistent Virtual Presence controls that continue to be
enforced -- to the extent required by the controls
themselves -- as protected **digital** content is, for example,
used and reused, copied and further distributed, extracted
and embedded, audited and reported;

persistency responsive to rules and controls associated
with **electronic** events, that causes new secure content
containers to be created automatically by systems and
methods supplying the procession of secure transport

vehicles required by Chain... ...audit information, and the
like;
securely generated containers carrying with them rules
and controls stipulated by rules and controls associated
with one or more triggered **electronic** events;
I 0 capabilities for persistency and independent secure
delivery and merging of rules and controls that provide
technical means for ensuring that dynamic user... ...discouraged;
dynamic user behavior encouraged as a critical link in
1 5 building ad hoc relationships and cost-effectively
distributing content, while simultaneously ensuring that
rights holders are protected and retain control over their
business models;
enabling ad hoc behavior that frees users from
constraints on their conduct resulting from inflexible,
first generation technologies;
support for enterprising behavior that is characteristic of
traditional commerce resulting in more efficient and
more satisfying **electronic** commerce experiences;
general purpose character **electronic** commerce
technologies provided by a combination of important
capabilities including component, object oriented,
programmable control language; secure specialized
container technology: independent delivery of secure
control...event driven
operating system functions; and the advanced security
architecture - allowing multiple simultaneous models to
I 0 evolve, and practically and efficiently operate;
general purpose **rights** and event management
architecture that is intrinsically reusable for many
simultaneous models -- providing enormous competitive
economic advantages over technologies that are
1 5 essentially single... ...design;
commerce architecture client nodes that are basic pieces
of reusable cyberspace infrastructure;
generalized configurability resulting, in part, from
decomposition of generalized requirements for
supporting **electronic** commerce and data security into a
broad range of constituent "atomic" and higher level
components (such as load modules, data elements, and
methods) that may be variously aggregated together to
form control methods for commercial **electronic**
agreements and data security arrangements;
a secure operating environment employing VDE
foundation elements along with securely deliverable
VDE components that enable **electronic** commerce

models and relationships to develop;

the unfolding of distribution models in which content providers, over time, can expressly agree to, or allow, subsequent content providers and/or users to participate in shaping the controls for, and consequences of, use of **electronic** content and/or appliances;

I 0 a very broad range of the functional attributes important for supporting simple to very complex **electronic** commerce and data security activities;

electronic information and/or appliance usage control (including distribution), security, usage auditing,

5 reporting, other administration, and payment arrangements;

capabilities that rationalize the support of **electronic** commerce and **electronic** transaction management stemming from the reusability of control structures and user interfaces for a wide variety of transaction management related activities;

content usage control, data security, information auditing, and **electronic** financial activities that can be supported with tools that are reusable, convenient, consistent, and familiar;

a general purpose **Rights** Operating System employing a reusable kernel and **rights** language components that provides the capabilities and integration needed for the advanced commerce operating systems of the future;

a general purpose, reusable **electronic** commerce capabilities that all participants can rely on will become as important as any other capability of operating

I 0 systems;

such a **rights** operating system providing **rights** and auditing operating system functions and other operating system functions -- the **rights** and auditing operating system functions securely handling tasks that relate to

1 5 virtual distribution environment;

secure processing units and/or protected processing environments that provide and/or support many of the security functions of the **rights** and auditing operating system functions;

an overall operating system designed from the beginning to include the **rights** and auditing operating system functions plus the other operating system functions -- or incorporation of the **rights** and auditing operating system functions as an add-on to a preexisting operating system providing the other operating system functions;

operating system integration and the...Figures 5-12 and the discussion above provide an

introduction
to the following detailed description of presently preferred
embodiments in accordance with these inventions. The "**electronic**
matchmaker" shown in Figures 5-12 is implemented in these more
detailed embodiments by a matching and classification utility system
900.

]Example Matching And Classification... ...al". Such objects may comprise information
and/or
1 5 associated rules for using the information. For example, object
classifier 902 may receive as inputs.

rights management information 909 such as rules
and/or associated consequences;
things 908 controlled or affected by such **rights**
management information including, for example
content objects or other information subject to such
rules;
items 9 1 0 such as metadata, abstracts or the like... ...to classify people. User classifier
904 can
classify people based, for example, on.

audit trails 912 indicating how people have used their
computers and other **electronic** appliances;
profiles 914 developed by asking users questions
I 0 about ...descriptors 910;
* content 950;
9 audit trail information 916;
e user information such as profiles 914;
0 Class information 952;
* user information 954;
9 other **rights** management information 956;
* matching criteria 958;
1 5 0 selection criteria 960; and/or
9 other information.

Matching and classification utility 900 in this example... ...or selecting processes;
reports 966 indicating the results of classification,
matching, and/or selecting processes;
targeted objects and/or pointers 968;
controls 909;
9 other **rights** management information; and
other classification, matching and/or selection related
information.

A Preferred Embodiment Matching and

Classification Utility 900 is a VDE-Aware Commerce
Utility... ...a commerce utility system 90 as described in
"Shear et al", and may comprise one or more processes securely
distributed over one or more secure **electronic** appliances within a
1 5 "Virtual Distribution Environment" as described in "Ginter et aFl.

Furthermore, the present inventions can be used in combination with
and/or make use of a wide array of distributed **electronic**
administrative and support services that may be referred to as the
"Distributed Commerce Utility." Such a Distributed Commerce
Utility may be, among other things, an integrated, modular array of
administrative and support services for **electronic** commerce and
electronic rights and transaction management. The Distributed
Commerce Utility provides, among other advantages, comprehensive,
integrated administrative and support services for secure **electronic**
commerce and other forms of **electronic** interaction. These
administrative and support services can be used to supply a secure
foundation for conducting financial management, **rights** management,
certificate authority, rules clearing, usage clearing, secure directory
services, and other transaction related capabilities functioning over a
vast **electronic** network such as the **Internet** and/or over organization
internal Intranets, or even in-home networks of **electronic** appliances.

Such **electronic** interactions supported by the Distributed Commerce
Utility may, for example, entail the broadest range of appliances and
distribution media, non-limiting examples of which include... ...CDROM and DVD in all
their current and future forms.

These administrative and support services can, for example, be
adapted to the specific needs of **electronic** commerce value chains in
1 5 any number of vertical markets, including a wide variety of
entertainment applications. **Electronic** commerce participants can, for
example, use these administrative and support services to support
their interests, and/or they can shape and reuse these services in
response to competitive business realities. Non-exhaustive examples
of **electronic** commerce participants include individual creators, film
and **music** studios, distributors, program aggregators, broadcasters,
and cable and satellite operators.

The Distributed Commerce Utility can, for example, make
optimally efficient use of commerce administration resources, and
can, in at least some embodiments, scale in a practical fashion to
optimally accommodate the demands of **electronic** commerce growth.

The Distributed Commerce Utility may, for example, comprise a
number of Commerce Utility Systems. These Commerce Utility

Systems can provide a **web** of infrastructure support available to, and reusable by, the entire **electronic** community and/or many or all of its participants. Different support functions can, for example, be collected together in hierarchical and/or in networked relationships... ...form different Commerce Utility Systems for different design implementations and purposes. These Commerce Utility Systems can, for example, be distributed across a large number of **electronic** appliances with varying degrees of distribution.

1 5 Such a "Distributed Commerce Utility" provides numerous additional capabilities and benefits that can be used in conjunction with the particular embodiments shown in the drawings of this application, non-exhaustive examples of which include.

- Enables practical and efficient **electronic** commerce and **rights** management.

. Provides services that securely administer and support **electronic** interactions and consequences.

Provides infrastructure for **electronic** commerce and other forms of human **electronic** interaction and relationships.

. Optimally applies the efficiencies of modern distributed computing and networking.

Provides **electronic** automation and distributed processing.

Supports **electronic** commerce and communications infrastructure that is modular, programmable, distributed and optimally computerized.

. Provides a comprehensive array of capabilities that can be combined to support services that perform various administrative and support roles.

. Maximizes benefits from **electronic** automation and distributed processing to produce optimal allocation and use of resources across a system or network.

1 5 Is efficient, flexible, cost effective, configurable...in combination with the inventions disclosed herein.

In more detail, as shown in Figure 14A, matching and classification utility 900 may include one or more **rights** operating system layers 90-1; one or more commerce utility support service

layers 90-4; one or more service application connect layers 90-3; and... ...processing
environments 154 may be used to support secure functions
90-D. Matching and classification utility 900 may be controlled, at
least in part, by **rights** management information such as for example.

VDE-compatible controls 909;
1 5 e rules and/or their consequences; and/or
other **rights** management information.

Matching and Classification Utility Can Interact
With Other Commerce Utility Systems
Figure 15 shows that matching and classification utility 900
can interact and interrelate with other commerce utility systems
described in "Shear et al" including for example.

financial clearinghouses 200,
usage clearinghouses 300,
rights and permissions clearinghouses 400,
certifying authorities 500,
secure directory services 600,
transaction authorities 700,
VDE administrators 800, and/or
* other commerce utility systems 90.

Figures... ...information, and/or
Other information.

Matching and classification utility 900 may receive from usage
I 0 clearinghouse 300.

requests for class information,
usage and/or **rights** management information,
audit records, and/or
other information.

Figure 15C shows example interaction between matching and
classification utility 900 and **rights** and permissions clearinghouse
400. In this example, **rights** and permissions clearinghouse 400 sends
matching and classification authority 900.

controls sets and/or object information;
e requests for class information;
clearinghouse usage data; and/or
other information.

In this example, matching and classification utility 900 sends

the **rights** and permissions clearinghouse 400.

rights management information such as control sets,
requests for information,
Class related information such as classes and/or class
assignments, and/or
* other information.

Figure 15D... ...sends the
VDE administrator 800.

requests for administration,
I 0 * Class related information such as classes and/or class
assignments,
requests for node and/or **web** information, and/or
other information.

In this example, the VDE administrator 600 sends the matching
1 5 and classification utility 900.

requests for classification information...manufacturing companies in the
Pacific rim." Organizations, such as companies, non-profit groups or
the like may have their own Commerce Utility Systems 156. Certain
electronic commerce or other activities (the entertainment industry,
I 0 for example) might have their own vertically-specialized Commerce
Utility Systems 158. Certain geographical, territorial orjurisdictional... ...transactions
being managed, and a variety of
other factors. Delegation of clearing authority may be partial (e.g.,
delegate usage aggregation but not financial or **rights** management
I 0 responsibilities), and may be consistent with peer-to-peer processing
(e.g., by placing some functions within consumers' **electronic**
appliances while keeping some other functions centralized).

Matching and Classification Utilities Can Provide
Services to Classes of Nodes, Users, Content Services
1 5 and/or...4 and 5 might have sub-types as well as
types.

A matching and classification utility 900 might break out along
content classes (e.g., **movies**; scientific, technical and medical; and
1 5 software). Subtype A might include first run **movies**, oldies, and art
films; subtype B might handle journals and textbooks; and type C
might be responsible for games, office, educational content. Peer-to
peer... ...such as for example.

automatic class generation,

automatic matching,
automatic class assignment,
class based searching,
class based directory,
audit by class,
market research,
I 0 **rights** management language processing,
other service functions.

Example Detailed Steps Carried Out By Matching
and Classification Utility System 900
1 5 The next section of the...categories developed by the classification method
that has been applied (Figure 18, block 1849; Figure 19, block 1849').

Finally, the process stores the results in **electronic** and/or non
electronic storage in the "write output data" step (Figure 18, block
1 5 1850; Figure 19, block 1850').

The "get input data" step 1840, 1840' may involve obtaining
attribute and/or parameter data from various sources including, for
example.

electronic appliance related attribute data;
9 user demographic data;
user psychographic data;
available **rights** management rules and/or consequences
(e.g., permissions records);
exercised **rights** management rules and/or consequences
(e.g., permissions records);
rights management and/or other audit and/or usage records;
any third party source of any information, including **rights**
management, usage, audit, statistical, personal,
organizational, political, economic, social, religious,
business, government, medical, research, academic, literary,
military, and/or information and/or data in any... ...process.

Figure 20 shows an example composite record 1852. This
composite classification record may contain attributes derived from
any or all of a variety of **rights** management and/or other data
"harvesting" processes. For example, composite record 1852 may
include demographic and/or psychographic data obtained by querying
the user 95. It may contain usage data obtained by monitoring audit
information produced by various usage transactions. It may contain
information reflecting user choices concerning **rights** management
information, the **rights** management information available to
particular users and/or objects, and **rights** management processes

actually performed with respect to particular users and/or particular objects. The information may be analyzed first to provide statistical and/or other summary information, or individual, more granular information may be provided. The composite record 1852 may also contain attributes of particular **electronic** appliance I 00 installations.

The particular example composite record 1852 shown in Figure 20 is one non-limiting example composite attribute record containing I 0...travel information, and generally do not participate in "pay per view" events and/or content consumption. Members of class I also tend to add new **rights** and/or modify existing **rights** management controls for content, for instance, to add a markup and **redistribute** the **content** in one example, may be less likely to express a religious preference and/or affiliation, and tend to use the **Internet** as an area for "surfing" and exploration.

Members of class 2 tend to pay less for content purchased, seldom travel abroad, tend to be interested in sports, religious content and events, and are more often consumers of **movies** than are members of class 1. Members of class 2 are more likely to "pay per view" than are members of class 1. and are much less likely to add new controls to content and/or modify **rights** acquired. Members of class 2 are more likely to express a religious preference and among those that do, Protestant denominations are more frequently mentioned. Members of class 2 may use the **Internet**, but tend to do so as part of their work role and responsibilities rather than as 1 5 entertainment, hobbies, and other leisure-time pursuits...Appliance Related Data Figure 24 shows example steps performed by the matching and classification utility 900 to collect appliance attribute data. In this example, an **electronic** appliance I 00 may have certain information associated with it. For example, a VDE administrator 800 may initialize appliance I 00 with certain information upon... ...processing the administrative event(s) using the 11create appliance attribute record" method to determine whether the administrator already has the desired information for the particular **electronic** appliance 100. If the operation is successful ("yes" exit to decision block 1512, Figure 24), the VDE administrator 800 may send, to the matching and... ...Figure 24), the "create I 0 appliance attribute record" method operating at VDE administrator 800 may, in this example, collect the data directly from the **electronic** appliance I 00 by sending ...place) perform block 1516 to send a container 152 with one or more administrative events and the "create appliance attribute record" method directly to the **electronic** appliance 100.

Figures 25(A) and 25(B) together show example steps

performed by the "create appliance attribute data" method shown in Figure 24, blocks... ...with the method. This example method (which, as explained above, may be performed by the matching and classification utility 900, the VDE administrator 800, the **electronic** appliance I 00, any other **electronic** appliance, or a combination of any or all of these) first locates the site configuration record(s) corresponding to the **electronic** appliance for which appliance attribute data is to be collected (Figure 24A, block 1522). This site configuration record(s) may, for example, be stored in the **electronic** 1 5 appliance secure database. The method next locates the permissions record for the site configuration record(s) (Figure 24A, block 1523).

The SPE next... ...audit record
(Figure 25A, block 1527).

After completing processing of site configuration records, the method then locates the user configuration record(s) corresponding to the **electronic** appliance for which appliance attribute data is to be collected (Figure 25B, block 1528). This user configuration record(s) may, for example, be stored in the **electronic** appliance secure I 0 database. The protected processing environment 154 next locates the permissions record for the user configuration record(s) (Figure 2513, ...events to activate such methods)
directly to the user 95 about which demographic information is to be collected (Figure 2713, block 1558). The user's **electronic** appliance 1 00 may, in response, process the one or more events using the "demographic data query" method, which may write an associated audit record... ...record (Figure 27B, block 1564@ 1566). If the required demographic data is successfully collected ("yes" exit to decision block 1562, Figure 27B), the user's **electronic** appliance may process one or more events using the "create demographic record" method supplied by step 1558, which may write an associated audit record (Figure 2713, block 1568). The **electronic** appliance may then send appropriate administrative events and the demographic attribute record to the matching and classification utility within one or more containers 152 (Figure...required data (Figure 30, block 1586). If the required data
is available from the repositories ("yes" exit to decision block 1588, Figure 30), then an **electronic** appliance at the repository (in this example) processes one or more events using the "create psychographic attribute record" method supplied by block 1586 in order...900
may, in response, send.one or more administrative events, a "collect psychographic data" and "create psychographic attribute record" method directly to the user's **electronic** appliance I 00 within one or more containers 152 (Figure 30, block 1596). The user's **electronic**

appliance I 00 may, in turn, process the events using the "collect psychographic data" and "create psychographic attribute record" methods (Figure 30, block 1598, 1600... ...and consequences. The matching and classification utility 900 may first send one or more administrative events and a "send permission records" method request to an **electronic** appliance 100 within one or more containers 152 (Figure 3 3, ...example, information from the permissions record header can be copied into the attribute record (Figure 35A, block 1634), and then the method may locate the **rights** record header 1 5 (block 1636, Figure 35A). Information from the **rights** record header may be copied into the attribute record (block 1638, Figure 35A), along with the identifier for the corresponding **right**(s) (blocks 1640, 1642, Figure 35A). The process may then recursively locate and harvest data from each method header contained within the **rights** record (blocks 1644, 1646, 1648, Figure 3513). The process may recursively repeat steps 1638-1648 for each **rights** record within the permissions record (as tested for by decision block 1650, Figure 3513). Finally, the ...record 1680-2 shown in Figure 37B includes, as a more detailed example, a user ID number field 1682, an object ID field 1684, a **right** ID field 1686a, a I 0 method identifier field 1686b, another **right** ID field 1686c, and corresponding method type fields 1686(d), a further **right** ID field 1686e and two corresponding method attribute fields 1686f, 1686g, a further **right** ID field 1686h and corresponding method attribute fields 1686i5 1686j.

Figure 37C shows a different example in coding for the Figure 37B example attribute record... ...for assembling rules and consequences. In this example, the matching and classification utility 900 may send one or more administrative events and a "get user **rights** table" method within a container 152 to an **electronic** appliance (Figure 3 8, block 1690). The **electronic** appliance I 00 processes the one or more events using the "get URT" method, which may writes an ...In this example, the matching and classification utility 900 sends one or more administrative events and a "create attribute record from URT" method to the **electronic** appliance I 00 that stores or has access to the user **rights** table information (Figure 39, block 1702). The appliance then processes the events using the method sent to it, and the method writes associated audit information... ...to decision block 1706, Figure 39, block 1708).

Figures 40A, 40B show example steps performed by blocks 17001 1704 to "create attribute record from user **rights** table." The method begins by checking associated permissions for the user **rights** table records (Figure 40A, block 1720). Assuming that appropriate

user and/or group permission is available, the method next locates the user **rights** table (Figure 40A, block 1722), and then begins 1 5 recursively analyzing the user **rights** table information to harvest desired attribute information from it (Figure 40A, blocks 1724 and following). In this particular example, the method locates the user **rights** table record (block 1724, Figure 40A, and then locates the first **rights** record header within the first user choice record within the URT record (blocks 1726, 1728, Figure 40A). The method copies **rights** record header information to the attribute record (block 1730), and then locates the **right** identifier and copies that to the attribute record (blocks 1732, 1734). The method then recursively locates each method header within the user **rights** table **right** record, and copies corresponding attribute information to the attribute record (blocks 1736, 1738, 1740, Figure 4013). Steps 1728-1740 are performed recursively for each **rights** record within the user choice record (see Figure 4013), decision block 1742), and the above steps are performed recursively for each user choice record within the user **rights** table (see decision block 1744, Figure 40B). Additionally, steps 1724-1744 are performed recursively for each user **rights** table record within the user **rights** table (see Figure 4013, decision block 1746). As a last example step, the method creates a permissions record that controls access and use of the... ...begin by locating a corresponding permissions record (Figure 41, block 1750) and then determining whether there is a permission record corresponding to the corresponding user **rights** table entry (Figure 41, decision block 1752). If there is no such entry (11nott exit to decision block 1752), the method may report failure, write... ...required permissions to enable usage ("yes" exit to decision block 1760, Figure 41), the method may access the permissions record (if any) for the user **rights** table for use in controlling access to the user **rights** table itself (block 1768, Figure 41).

Figures 42A-42C show example **rights** attributes records 1770 that may be obtained from the processes above. The Figure 42A example **rights** attribute record 1770-1 includes a user or group ID I 0 field 1772, an object ID field 1774, and any number of attribute fields 1776(1)5 ... . 1776(n). The more detailed example **rights** attribute record 1770-2@ shown in Figure 42B includes a user ID number field 1772, an object ID field 1774, a **right** ID field 1776a and corresponding method attribute field 1776b, another **right** ID field 1 5 1776c and corresponding method attribute field 1776d, a **right** ID field 1776e and corresponding method attribute fields 1776f, 1776g, and another **right** ID field 1776h and corresponding method attribute field 1776i.

Figure 42C shows how the **rights** attribute record 1770 can be
encoded numerically as opposed to using characters, as one example.

Example Steps for Assembling Usage Audit Records
Figure 43 shows...44 example, the matching and
classification utility 900 sends one or more administrative events and
a "create attribute record from audit record" method to an **electronic**
appliance I 00 within one or more containers 152 (Figure 44, block
1792). The appliance I 00 may then process the one or more
administrative...1836(1), ... ,
1836(n). The more detailed Figure 46B example attribute record
1830-2 includes a user ID number 1832, an object ID 1834, a **right** ID
1836a and associated method characteristic 1836b, another **right** ID
1836c and associated method 1836d and associated statistic 1836e, a
further **right** ID 1836f and associated method attribute 1836g, another
right ID 1836h and associated methods 1836i, 1836j, and associated
additional attributes 1836k-1 836o. The characteristics shown in
fields 1836k-1836o could, for example, be... ...transactions, and other events on the
inefficient, these search activities share in common the feature that
each consumer must intentionally "pull" desired content from a **Web**
site to their computer after successfully identifying specific content or
services of interest at that time. The present inventions also support
"pull" models-a topic... ...e.g., a protected processing environment 154) installed on their
I 0 appliances. These example appliances may be of any kind, including
computers, so-called **Web** television or **Web**-TV, DVD appliances
with some form of backchannel, a settop box with a "back channel",
and so on.

Perhaps with the permission of the user... ...all or a portion of these audit records in a
VDE
container 2008 to the matching and classification utility 900. The
audit records may contain **rights** management information, including,
but not limited to the amount of usage, the amount paid, if any, the
payment method used, if any, VDE control sets...create at least
one object class hierarchy, object class, object classification scheme,
object category and/or object category scheme using at least some
1 5 **rights** management information and assign at least one object to at
least one category and/or class.

The matching and classification utility 900 takes the usage
information and other **rights** management information received from
the VDE nodes and/or other information sources and may create at
least one category and may assign at least one... ...In Figure 47, the matching and
classification
utility 900 sends a VDE container 2002 to content provider 201 0 with
information showing the classes of **content used** by one or more nodes

and/or users along with a request that the provider 20 1 0 send similar
content back to one or... ...available content that may be of
interest to user A given the history of content usage as reflected in
VDE audit records and/or other **rights** management information. In
this "push" example, classes of content or information about available
content may be pushed automatically from (a class of) content
providers to... ...for
I 0 content of interest to them.

In this example, user A receives content that may be most like
content the user has already **used**, perhaps like **content used** most
frequently in the recent past. The present inventions also support the
matching and classification utility 900 and/or content provider
1 5 sending content...apparent interests to
determine if the user's circle of interest might be a little larger than
that indicated by past usage and other, related **rights** management
information alone.

In another example, providers may from time to time send
content unrelated to the user's apparent interests that may
nevertheless reflect... ...by sending a VDE container with
1 5 appropriate user and content class information, suggest to a provider
that user A receive content similar to **content used** by another member
or members in the same group or class as user A. In one example, the
matching and classification utility 900 may suggest... ...arrangements may include
appliances such as a WebTV interface
and/or an intelligent "settop box" connected to an interface device
that uses one or more (**digital**) TVs for display. Still other
arrangements may include an NC computer without a local hard disk
I 0 logically connected to at least one server, a personal **digital** assistant
with a network connection, and/or any other appliances with suitable
processing, storage, and communications capabilities.

Referring again to Figure 47A, each customer appliance... ...as on the same local area
network, and/or may be distributed across
wide area networks such as multi-location corporate Intranets and/or
the **Internet** itself. Among other tasks, messaging services 2058
"listens" for messages destined for that particular appliance or for
broadcast messages intended ...the US market share of PC vendors,
information in text format, costing less than a dollar per item, and for
which the subscriber receives the **right** to excerpt at least one whole
paragraph, provided that the excerpted amount constitutes less than
25% of the entire item based on word count." This...1 0 create at least one object class
hierarchy, object class, object
classification scheme, object category and/or object category scheme
using at least some **rights** management information and assign at least

one object, item, and/or subscriber to at least one category and/or class.

1 5 Subsequent to receipt...set of rules and usage consequences that apply to members of one or more item classes, thus potentially improving the efficiency of distribution and of **rights** management. In another example, the rules and content items may be sent in separate VDE containers. In this example, the messaging services 2058 and subject... ...may be installed and run on network routers, network switches, one non-limiting example being ATM switches, and other packet and/or cell switches.

Example: **Digital** Broadcasting Based On Matching And Classification
"Shear et al" discloses a **Digital** Broadcasting Network ("DBN") that may function as a cooperative of **Web** sites and, for example, service providers, with a central and perhaps regional and logical (e.g., market based) headquarters groups, or it may function as... ...a "higher" level cooperative or corporation.

Figure 48 shows one non-limiting example 2 1 00 of a DBN that includes one or more DBN **Web** servers 2104(l)-2104(n) and one or more **Web** users each with VDE nodes. Users are attracted to a specific DBN server (or servers) because it provides access to specialized content and/or services 2108. Based at least in part on **rights** management information 21 1 0 collected from DBN servers, for example, controls associated with the most frequently requested information, the matching and classification ...classification utility 900 may may create at least one class
hierarchy, class, classification scheme, category and/or category I 0 scheme using at least some **rights** management information and assign at least DBN server and/or at least some information to at least one category and/or class.

For example, one... ...same. The request may be sent independently of the class information.

In another example, the matching and classification utility 900 may receive content and/or **rights** management information from providers and go on to create classes of content and/or content providers in which the classes may be partly defined using **rights** management data. Content on one class may, among other things, be distinguished from content in another class by price, payment methods, usage opportunities (e.g example Figure 48 shows that the DBN 21 00 may consist of video 2202 and/or **audio** 2203 content providers who send certain categories of video and/or **audio** content 2206 to DBN servers

2204(l)-2204(n) based on the categories of content each server may specialize in, which, in turn, may be determined at least in part on I 0 frequency of usage and/or other **rights** management information sent in VDE containers 2213 to the matching and classification utility 900, or to a usage clearinghouse 300 and then to a matching... ...send content in specific categories 2206 to specific DBN servers 2204. In turn, each DBN server 2204(l)-2204(n) delivers video 2208 and/or **audio** 2209 in VDE containers to parties interested in such content. In another example, a VDE container may hold both video and **audio** and/or any other content type.

Example: Matching and Classification Utility 900
Can Also Support "Pull" Distribution Models Based
On Classes
Notwithstanding the noted trend... ...or node. The classification method may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least one service and/or at least some content to at least one category and/or class.

Subsequently, a VDE...These commerce utility systems and servers are also connected to the company Intranet 2418. The company 2406 also maintains one or more connects to the **Internet** 2402. (In another example the company may maintain connections to at least one private network operated by themselves and/or another party in 1 5 addition to, or instead of one or more connections to the public **Internet**.) The content server(s) may provide access to internal, proprietary company information and/or to external, often commercial information. The internal content server may act... ...2404(A)-2404(C) and/or may host commercial content locally on a content server 2408.

In one example, VDE audit records and/or other **rights** management information are sent in VDE containers 2412 from one or more VDE nodes 2420 to the enterprise usage clearinghouse 300 which may forward at... ...containers2410totheenterprisematchin andclassificationutility 9 900. The enterprise matching and classification utility 900 may also collect from internal information sources 2414 information in addition to audit and **rights** management information, such as information in a human resources, accounting, and/or budgeting database containing data about company employees. These data may indicate, in one...matching and classification utility 900 may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least service and/or at least some content to at least one

category and/or class.

1 5 In one example, using at least some VDE **rights** management
data, for example, whether certain information can be viewed by
anyone, by any employee, or only by employees in certain job
classes, such as... ...and/or responsibilities.

In turn, the enterprise matching and classification utility 900
sends to at least one external content and/or service provider 2404 on
Internet 2402 one or more VDE containers 2424 with information that
indicates categories of interest. The content providers 2404 may
themselves be specialized; in one example...of rules and usage consequences that may
vary
according to class. In this non-limiting example, the class is "content
type." The publisher may have **rights** in a wide variety of content and
content types. Consequently, the publisher may create rules for text
objects that may differ from rules for **audio** objects.

The publisher 2502 sends the class-based rules and usage
consequences to a first creator 2504 who also has installed VDE on
her or his appliance 2516 and who has also been given one or more
certificates and/or other **digital** credentials by the publisher (and/or
trusted third party) indicating that he is indeed a creator authorized by
the publisher 2502. The publisher has included... ...adds a text
file to the container 2520 along with her rules and usage
consequences. As before, she also has a certificate and/or other
digital credential(s) identifying her as authorized by publisher ABC to
add and/or modify content and rules and usage consequences. As in
the case of...and usage
consequences to a matching and classification authority 900 who may
classify the rules and send the rules and their class assignments to a
rights and permissions clearinghouse 400. The matching and
classification utility 900 may also create at least one class hierarchy,
class, classification scheme, category and/or category scheme using at
least some **rights** management information and assign at least one rule
to at least one category and/or class.

An authorized first creator 2604 may send a VDE container
2617 to the **rights** and permissions clearinghouse 400 asking for rules
in the class "rules for authorized creators, for image objects, from
publisher ABC." The **rights** and permissions clearinghouse 400
returns a VDE container 2614 with rules in the requested class. The
first creator 2604 uses a packaging application 2616 to package his
image using these rules plus rules and usage consequences reflecting
his **rights** and wishes and sends the VDE container 2614 to the second
creator 2606.

The second creator 2606 also sends a VDE container 2619 to the **rights** and permissions clearinghouse 400 asking for rules and consequences in the class "rules for authorized creators, for text 1 5 objects, from publisher ABC." The **rights** and permissions clearinghouse 400 returns a VDE container 2621 with rules and consequences in the desired class. The second creator 2606 uses a packaging application... ...individuals, organizations, groups, and/or other classes. Examples of these industries include direct marketing, advertising, yellow and white pages directories, directories of directories, and various **electronic** and paper membership lists and professional directories.

In addition to identifying information such as names, e-mail addresses, physical mailing addresses, phone numbers, fax numbers...in class "AF." The requested class could be any class defined by one or more attributes and may be based on usage profiles that include **rights** management information, non-exhaustive examples of which include price, payment methods accepted, permitted operations, meters, and privacy controls.

The secure directory services 600 returns to... ...certain combinations of leisure-time activities. These classes might have been defined at least I 0 in part on the basis of usage and other **rights** management information 2816, for example, the kind of leisure-time information recently looked at, for how long, and/or its cost, and/or the kind of **Web** sites recently frequented, sent from consumer VDE nodes 2802(l)-2802(n) to the matching and classification utility 900, and/or to a usage 1...matching and classification utility 900 may also create at least one class hierarchy, class, classification scheme, category and/or category scheme using at least some **rights** management information and assign at least one consumer, service, and/or at least some information to at least one category and/or class.

Example Figure 53 shows that a consumer 2802(l) has recently indicated a preference and/or interest in skiing, **music**, and flying to Colorado. Another consumer 2802(n) has indicated a preference for and/or interest in surfing Hawaii. These preferences may be determined at least in part on the basis of **rights** management information. In response queries sent in one or more VDE containers 2 8 1 0 from the travel company asking for interest and preference... ...VDE containers 2806 to the travel company 2801 indicating agreement to buy the package offered or 1 5 may request additional information or may negotiate **terms** and conditions such as price, departure date, insurance, and the like.

These negotiations may be conducted using the inventions described
in "Ginter et al", Figures...then send a VDE container 291 0 to a
matching and classification utility 900 with a query asking who can
supply the desired items under **terms** and conditions that are also
included in the container. Since these **terms** and conditions may be
the subject of negotiations, they may be in a format conducive to
VDE-based negotiations as described in "Ginter et al... ...sends at least one VDE
container 2918 to buyer A 2904 indicating
that they will sell buyer A the previously requested items under the
enclosed **terms** and conditions. In another example, there may be
I 0 some VDE-based (see "Ginter et al", Figures 75A-76B) negotiations
between the various parties... ...index
information, financial performance data for publicly held companies,
forecasts, risk management information, options and futures, and the
like. The classification method may also utilize **rights** and
permissions, including access control information, permitted
operations, and/or expiration times and/or dates for **rights**
management information. The classification method may also create
at least one class hierarchy, class, classification scheme, category
and/or category scheme using at least some **rights** management
information and assign at least one element to at least one category
I 0 and/or class.

In turn, using the VDE aware appliance...matching and classification utility 900 may also create at
least one class hierarchy, class, classification scheme, category and/or
category scheme using at least some **rights** management information
and assign at least some trading information to at least one category
and/or class.

The example trader 3102 examines the recommendation and...classification authority 900 asking,
"which banks are in class A?," where class A are "those banks that
offer the highest savings interest, no ATM fees, **online/Web** banking
using VDE, insured accounts, free checking with balances larger than
$2,500, "image" statements (where check images rather than the
actual checks are returned...Among the ways in VDE nodes, users, content services, and/or
transaction services can be authenticated is through the use of
certificates and/or other **digital** credentials issued by an appropriate
trusted third party, a certifying authority 500, for instance, that
warrants and/or attests to some fact or facts,, which... ...authority 900(1 -N)s, each of which may
provide its services to different classes, where class membership is
authenticated using certificates and/or other **digital** credentials. In
other examples, additional authentication mechanisms may be used in

combination with, or instead of certificates, such as information
known only to the user... ...consequences conditional on class definitions and/or the assignment
of members to a class. Class membership may be authenticated by a
certificate and/or other **digital** credential issued by one or more
commerce participants in addition to, and/or instead of a trusted third
party such as a certifying authority 500. For example, a certificate
1 5 and/or other **digital** credential may attest to user identity, that is, that a
user is the user he or she claims to be. Nodes, devices, networks,
servers, clients, and services, are other non-limiting examples of other
commerce elements that may be authenticated with certificates and/ or
other **digital** credentials. Any commerce participant may issue a
certificate, but other participants are not required to accept a given
certificate as an authenticator.

Figure 59 shows... ...I 0 of these instances, the services of the matching and classification
authority 900 may depend upon finding certain authenticating
certificate(s) and/or other **digital** credentials on the appropriate VDE
nodes.

For example, matching and classification utility 900(1)
1 5 provides services to nodes 3410(1-n) in the... ...3412 issued by certifying authority 500(1) that provides
services to this deployment.

In another example, certifying authority 500(2) provides
certificates and/or other **digital** credentials to participants in a higher
education value chain 3404 consisting of an arbitrary number of
colleges and universities 3416(1)-3416(n), providers 3418... ...users and/or consumers of business information
I 0 3422(1)-3422(n), and a certifying authority 500(3) that issues
certificates and/or other **digital** credentials to members of the value
chain 3406.

In addition to membership in certain deployment, institutional,
and/or content usage classes, the matching and classification... ...3428(1)-3428(n) and one or more trading
companies 3430(1)-3430(n). In another example, other participants
may receive certificates and/or other **digital** credentials, including
banks and financial institutions, government authorities, for example,
tax and/or customs authorities, ...a commerce utility system may provide
services to more than one class where class membership is indicated
by at least one certificate and/or other **digital** credential issued by a
certifying authority 500 and/or value chain participant. In one
example, matching and classification authority 900 might provide
services to the class "Higher Education" and to the class "K-12

I 0 Education."
Possession of a certificate and/or other **digital** credential may
be among the information used to classify a node, user, appliance,
device, entity, and/or other commerce participant, and rules and
consequences can... ...more
1 5 authenticated classes and/or on the degree of confidence the rule
provider has in the trustedness of the certificate and/or other **digital**
credential issuer. In one example, a discount to higher education may
be larger if the root for chain of trust for a given certificate is... ...or
classes.

Example: Matching And Classification Authority 900
Supports Control Sets Based In Part On Employee
Classes, Content Classes, And/Or Certificates And/or
Other **Digital** Credentials
Chain of handling and control enables, amongst other things,
multiple organizations to work together in secure, trusted, efficient,
cooperative commerce processes. One way in... ...the class assignment of individual
and/or groups of
employees. In part by virtue of their employee classification, at least
one employee may receive certain **rights** management information,
for example, permission to access certain classes of information or
permission to perform one or more permitted operations, transactions
and/or events.

Example...or
other class definitions that apply to employees, members, and/or
others associated, affiliated, and/or employed by the organization,
group, entity and/or institution. **Rights** management information may
be part of the claim definition, for example, permissions to view,
modify, excerpt, and so on.

Control sets may provide permissions conditional... ...employees may modify certain
I 0 information and/or classes of information in a database while others
may not. Class membership may be indicated by **digital** credentials,
non-limiting examples of which include **digital** certificates and **digital**
membership cards. Controls may be conditional on other information
as well, for example, some computers and/or display devices may not
1 5 show certain... ...In another
example, this certificate and/or one or more additional certificates
may attest to the fact that the insurance company has the appropriate
charter, **licenses**, and other grants of authority to be in the health
insurance business. The certifying authority 500(1) may also send a
certificate in a VDE... ...identity. In
another example, this certificate and/or one or more additional
certificates may attest to the fact that the hospital has the appropriate

charter, **licenses**, and other grants of authority to provide hospital and related services.

The insurance company 3508 may have sent one or more control sets to the...be
1 5 treated as members of classes that define permissions, such as "confidential," "secret," "top secret," and so on. Other non-limiting example governmental **rights** may address permissions for import, use, and/or export of certain classes of hard goods, services, currency and financial instruments, and content. Travelers entering the... ...Children, for example, may be prohibited as a matter of law by governments from viewing content in the class "sexually explicit."
Another example of government **rights** is that different tax rules may be applied to different classes of **electronic** commerce transactions using VDE. Example 3700, Figure 62A-62B, shows a certifying authority 500 operated by and/or on behalf of a government issuing a certificate and/or other **digital** credential indicating jurisdiction, namely, country. The certificate is sent in a VDE container3710(a)toaVDEadministrator8OO. Thegovernment certifying authority 500 also sends certificates in VDE containers... ...certificates. The tax class
definitions 3712, tax control sets 3714, and government authority certificates 3716' are sent in at least one VDE container to a **rights** and permissions clearinghouse 400, who, in one example, redistributes the tax class definitions 3712(l), tax class control sets 3714(l), and/or government authorization... ...content of any kind, the appropriate tax control sets 3714(A) are also included in the VDE container. A tax control set is applied whenever **content** is **used** in accordance with a tax class and provided that the appropriate jurisdictional certificate
3 7 1 O' is present on the VDE node 3 706...The class assigned to each story may be carried in the container
as metadata for one or more story objects in another example. An example **Web** browser may request of the information provider an image appropriate to that class, which if available, would be sent in another VDE container.

Class may affect display rules in other example ways as well.

For instance, several team sports news stories may be displayed in a **Web** browser window in which a scene from a football or basketball game ...reads at less than the 4th grade level, the charge is only 40 cents. "Reading level" may be indicated by a certificate and/or other **digital** credential.

A matching and classification utility 900 may send administrative events and/or classification methods 3910 to

information providers, one or more other value chain...in a
VDE container 4006 at least one Uniform Resource Locator (URL)
that points to the location of the document(s) on the World Wide
Web.

The user 4002 in this example sends a message in a VDE
container 4008 asking for the document identified in the URL. A
provider sends...value chain
participant, or may have resulted more automatically from the
analysis by a matching and classification utility 900 of usage, audit,
and/or other **rights** management information and/or of "info exhaust,"
and/or of preference, demographic, and/or psychographic data and/or
classes of data.

In another example, the...And/Or Other Object Metadata
Among the numerous advantages of the present inventions is
the ability to create classes of classes based in part on **rights**
management information. The feature may enhance search efficiency
by enabling search engines to locate members of classes provided by
any of numerous schemes for object naming and object metadata that
have been proposed. For example, the IETF Uniform Resource
Locator (URL), the International Standard **Book** Number (ISBN),
International Standard Serial Number (ISSN), MARC library catalog
records, and the recent proposed "Dublin Core"(Weibel, Stuart, Jean
Godby, Eric Miller, and Ron... ...and classification utility 900 which (example step "2")
may create
new "classes of classes" 4306. These new classes 4306 are then made
available on a **Web** page 4308 (example step "Y) to interested parties
who may then search for objects according to their membership in
one (or more) of these new classes of classes. In example step "4" an
interested party 4320 sends a VDE container with a request to retrieve
the **Web** page 4308 with the classes of metadata information. The
Web server (in example step "5") returns a copy of the page 4312 to
the interested user 4320, who (in example step "6") sends a VDE... ...location
information for at least one member of the desired class(es) in the list
in container 4316.

Example: Matching and Classification Utility 900
Supports **Electronic** Gambling
Electronic gambling may be among the services that will drive
Internet growth in coming years. Such services raise many questions
for both providers and for users or players of the service. For
example, providers want to...example, players may be particularly interested in
the odds at the game of blackjack. In one example, a player may
prefer playing with a single **digital** deck of 52 cards and a particular
number of (emulated) shuffles rather than with say four decks and

more shuffles, the affect of the latter... ...play may consist of a series of
communications in VDE containers between the gambling provider
and the gambler.

Example: Matching and classification utility 900
Supports **Electronic** Ticket Sales and Distribution
The performing arts, exhibitions, theaters, and conferences are
some non-limiting examples of events that may require tickets for
admission. **Electronic** ticket agencies on the **Internet** and other
electronic arenas provide a connection between the consumer and
producers of the event. Consumers may want to know such
information as the nature of the event...ticket purchase at a given price, location, date,
event, and/or using a particular payment method.

1 5 In another example, the tickets may be **digital** and may have
associated with them one or more "seals", **digital** signatures, and/or
certificates indicating the authenticity and/or integrity of the **digital**
tickets.

While the inventions have been described in connection with
what is presently considered to be the most practical and preferred
embodiments, the inventions are...

Claims:

...category scheme and/or said assignment,
wherein at least one of said steps (a)-(c) includes the step ofI I using at least some **rights**
management information.
2 A method as in claim I wherein said using step includes
using at least one control set.
3 A method as in claim I wherein said using step includes
using at least some information for controlling use of **digital**information.
4 A method as in claim 1 wherein said using step includes
using at least some information for controlling at least onetransaction.
5... ...event.

6 A method as in claim I wherein said using step includes
using at least some information for controlling at least oneconsequence of **digital**
information use.
7 A method as in claim I wherein said using step includes
using at least some information for controlling at least oneconsequence... ...of at least one
transaction.
9 A method as in claim I wherein said using step includes
using at least some information outputted by a **rights** managementprocess.I 10. A method
as in claim I further including the step ofoutputting at least some **rights** management

information. I 11. A method as in claim I wherein at least one of steps (a)(c) includes using at least one secure container...said class, class hierarchy, classification scheme, categoryI 0 or category scheme and/or said assignment,I I wherein said system uses at least some **rights** managementinformation.

17 A system including:
first means for determining at least one class, class hierarchy,classification scheme, category or category scheme;second means for... ...category scheme and/or saidI 0 assignment,I I wherein at least one of said first, second and third means usesat least some **rights** management information.

18 A Commerce Utility System providing a secure
execution space, the Commerce Utility System performing at leastone component based service function including... ...for execution within the secure execution space, theCommerce Utility System including a communications facilitypermitting communication of secure control information with at leastone **electronic** community participant,wherein said component based service function uses at leastone class based at least in part on **rights** management information.

19 A Commerce Utility System as in claim 18 wherein the
component based service function assigns at least one member to atleast one class based at least in part on some **rights** managementinformation.

20 A Commerce Utility System as in claim 18 wherein the
component based service function matches persons and/or thingsbased at least in part on at least some **rights** management information.

21 A Commerce Utility System as in claim 18 wherein the
component based service function selects persons and/or things basedat least in part on at least some **rights** management information.

22 A Commerce Utility System as in claim 18 wherein the
component based service function narrowcasts information torecipients based at least in part on at least some **rights** managementinformation.

23 A system or method including:
a computer network anda control arrangement within the network that determinesand/or uses at least one of the following through use of **rights**management information:(a) class hierarchy,(b) class structure,(c) classification scheme,(d) category, andI 0 (e) category scheme.

24 A class-based system including at least one computer
that processes **digital** information, said system including at least oneelement that uses at least some **rights** management information.

25 A method of operating a class-based system including at
least one computer that processes **digital** information, said methodincluding the step of using at least some **rights** managementinformation.

26 A system for assigning at least one thing or person to at
least one class including at least one computer that processes **digital**information, said system including at least one element that uses atleast some **rights** management data in making said assignment.

27 A system for making and/or using at least one class
based assignment including at least one computer that processes**digital** information, said system including at least one element thatuses at least some **rights** management

information.

28 A system for clearing at least one transaction including at
least one computer that processes **digital** information, said systemincluding at least one element that uses at least one class defined,assigned, selected, and/or matched based at least in part on **rights**management information.

29 A method for authorizing at least one computer and/or
computer user including the step of using at least one class defined,assigned, selected, and/or matched based at least in part on **rights**management information.

30 A method for authorizing at least one **electronic**
transaction including the step of using at least one class defined,assigned, selected, and/or matched based at least in part on **rights**management information.

31 A method for initiating and/or performing at least one at
least in part secure **electronic** transaction including the step of usingclass related information defined, assigned, selected, and/or matchedbased at least in part on **rights** management information.

32 An information processing method including the steps
of.securely charging a fee; andconditioning said charging step at least in part on at least oneclass defined, assigned, selected, and/or matched based at least in parton **rights** management information.

33 A method for securely exchanging **digital** information
including the step of at least in part defining, assigning, selecting,and/or matching at least one class based at least in part on **rights**management information.

34 A method for performing at least one **rights** operating
system based transaction including the step of defining, assigning,selecting, and/or matching at least one class based at least in part on**rights** management information.

35 A method for performing at least one protected
processing environment operation including the step of defining,assigning, selecting, and/or matching at least one class based at leastin part on **rights** management information.

36 A method of pushing information including the steps of
classifying recipients and/or information to be sent to said recipientsbased at least in part on **rights** management information, and selectingsaid information to distribute to said recipients based at least in parton said classifying.

37 A method of pushing information including the steps of
classifying recipients and/or information to be sent to said recipientsbased at least in part on **rights** management information, andmatching at least a portion of said information with at least one classof said recipients based at least in part on... ...A method of pushing information as in claim 37 furtherincluding the step of creating a classification scheme and/or hierarchyusing at least some **rights** information.

39 A method of pushing information as in claim 37 further
including the step of assigning at least some information and/or atleast one recipient to a class or category, said assignment based atleast in part on **rights** management information.

40 A subject switch for matching subscribers and/or
recipients desiring information in one or more classes with one ormore sources of... ...subject switch matches atleast one subscriber and/or participant with at least one

informationsource on a mapping based at least in part on **rights** managementinformation.

41 A subject switch as in claim 40 wherein said information
source:selects at least some information, said selection based on atleast one class, and wherein said assignment of said at least someinformation to said at least one class is based at least in part on **rights**management information; andsends at least some said selected information to said subscriberin accordance with said subscriber's subscribing to said class ofinformation... ...least one computer providing aprotected processing environment.

43 A subject switch as in claim 40 wherein at least one
subscriber and/or participant uses **rights** management information atleast in part to persistently subscribe to at least some informationprovided by at least one information source.

44 A subject switch...said
subscriber and/or participant and said information source and/orparticipant to communicate electronically.

47 A subject switch as in claim 46 wherein said **electronic**
communications uses at least one secure container.

48 A subject switch as in claim 40 wherein at least one of
said subject switch, subscriber, or information source uses at least onecontrol set associated with at least some information received by atleast one subscriber.

49 A **digital** narrowcasting arrangement comprising:
a computer; andat least one classifying element **used** to select **content** tonarrowcast to recipients based at least in part on **rights** managementinformation.

50 A **digital** narrowcasting arrangement as in claim 49
wherein the classifying element classifies at least one of (a) arecipient, and (b) content, based at least in part on **rights** managementinformation.

51 A **digital** narrowcasting arrangement as in claim 49
wherein said classifying element defines at least one class using atleast some **rights** management information.

52 A **digital** narrowcasting arrangement as in claim 49
wherein the classifying element assigns at least some content to atleast one class, said assignment based on at least some **rights**management information.

53 A **digital** narrowcasting arrangement as in claim 49
wherein the classifying element defines at least one class based atleast in part on content selections previously made by the recipientsand/or profiles generated based at least in part on recipient input.

54 A **digital** narrowcasting arrangement as in claim 49
wherein the classifying element sends a content request includingclassification data and destination information to at least oneprovider... ...system including: acomputer network; and a selection arrangement that selectsinformation for use by individual recipients using classes based atleast in part on **rights** management information.

56 An information distribution system as in claim 55
wherein the system further includes a classifying element thatdetermines at least one class... ...least one recipient.

57 An information distribution system as in claim 56
wherein said classifying element defines at least one class using atleast some **rights**

management information.

58 An information distribution system as in claim 56
wherein said classifying element assigns at least some content to atleast one class, said assignment based on at least some **rights**management information.

59 An information distribution system as in claim 55
wherein the system includes means for allowing the user to choose toreceive the selected information.

60 An enterprise information system including a computer
system for classifying employees, said system including at least one**rights** management component that distributes information to theemployees based at least in part on employee classification.

61 An enterprise information system as in claim 60...A microsegmented merchandising technique as in claim

71 wherein the performing step includes defining at least one classhierarchy based at least in part on **rights** management information.

73 A microsegmented merchandising technique as in claim

71 further including the step of combining plural offers for differentproducts and/or services based at least in part on said classification.

74 A trading network including:
a communications element for communicating **digital** signals;andmeans for matching value chain participants through aclassification based at least in part on **rights** managementinformation.

75 A trading network as in claim 74 further including means
for defining at least one class hierarchy based at least in part on **rights** management information.

76 A trading network as in claim 74 further including means
for determining class membership based at least in part on action ...chain participant.

77 A trading network as in claim 74 wherein said matching
means includes means for at least in part performing at least one**electronic** negotiation.

78 A securities trading method including the step of
performing a classification process at least in part using at least one**rights** management element, and using the classification process toselect securities for trade.

79 A securities trading method as in claim 78 wherein said
classification process includes defining at least one class hierarchybased at least in part on **rights** management information.

80 A currency/debt trading system including:
a currency or debt trading computer; andan arrangement coupled to said computer that performs at leastone classification process based at least in part on **rights** managementinformation.

81 A currency/debt trading system as in claim 80 wherein
said arrangement includes means for defining at least one classhierarchy based at least in part on **rights** management information.

82 A currency/debt trading system as in claim 80 wherein
the arrangement uses classification to maximize return or minimizeloss..

83 A financial institution selection system including a
computer that classifies financial institutions based at least in part on **rights** management

information.
84 A software distribution method including the steps of
generating class information based at least in part on **rights**management information, and selecting software to be distributedand/or recipients who are to receive distributed software based at leastin part on class information.
85 A software distribution method as in claim 84 wherein
said generating step includes defining a class hierarchy using at leastsome **rights** management information.
86 A software distribution method as in claim 84 wherein
the selecting step includes selecting software to be distributed byclassifying the software based at least in part on **rights** managementinformation associated with the software.
87 A software distribution mehtod as in claim 80 wherein
the selecting step includes selecting recipients to receive softwarebased at least in part on usage information provided by a **rights**management process.
88 A classification technique including the step of
authenticating class membership based at least in part on **digital**credentials and/or certificates.
89 A classification technique as in claim 88 wherein said
digital credentials are **digital** certificates.
90 A classification technique as in claim 88 wherein said
digital credentials are **digital** membership cards.
91 A classification technique as in claim 88 further
including the step of deciding class membership based at least in parton **rights** management information.
92 A classification technique as in claim 88 further
including the step of classifying at least one of users, nodes, devices,networks, servers, clients and services based at least in part on **rights**management information.
93 A classification technique as in claim 88 further
including the step of conditioning at least one **rights** managementprocess at least in part on authenticated class membership.
94 A computer system including:
a first arrangement that generates class-based ...or services based on participants' classes.
96 A health care computer system including an arrangement
for issuing health care workers, administrators and insurers classbased **digital** credentials and/or certificates, wherein the **digital**information sent to said health care workers and administratorsincludes class-based controls that condition use and/or access toinformation based at least in part on said class-based **digital**credentials and/or certificates.
97 A health care computer system as in claim 96 further
including means for allowing said health care workers, administratorsand... ...in claim 98wherein said matching and/or classification computer includes meansfor defining at least one class hierarchy based at least in part on **rights** management information.I 100.
A work process automation system as in claim 98wherein said matching and/or classification computer includes meansfor matching based at least in part on **rights** management information.I 101. An automatic governmental and/or societal **rights**supporting system including a matching and/or classificationcomputing element

that assigns and/or classifies entities to at leastone class based at least in part on **rights** management information.102. An automatic governmental and/or societal **rights**supporting system as in claim 1 0 1 wherein the matching and/orclassification computing element includes means for defining a classhierarchy based at least in part on **rights** management information.103. An automatic governmental and/or societal **rights**supporting system as in claim IO 1 wherein the matching and/orclassification computing element includes means for classifyingentities based on at least one of the following:tax status;**right** to receive certain information;**right** to engage in certain transactions; andjurisdiction.104. An automatic taxing authority computer includingmeans for issuing tax class control sets based at least in...least in part onsaid classification.117. An information searching mechanism including amatching computer element that classifies information based at leastin part on **rights** management information, said computing elementincluding means responsive to user requests to search for informationbased at least in part on said classification.118. An... ...mechanism as in claim II 7wherein said matching computer element further includes means forassigning information to classes based at least in part on **rights**management information.119. An information searching mechanism as in claim II 7wherein said matching computer element includes means for scoringinformation based at least...An information classification method including the stepof generating at least one class hierarchy from other pluralclassification hierarchies based at least in part on **rights** managementinformation and/or class-based **rights** management information basedat least in part on classification metadata.126. An information classification method as in claim 125further including basing said other plural... ...name,prices, permissions, ISSN, title, author, publisher and/or date.128. An information classification method as in claim 125further including generating said class-based **rights** managementinformation by classifying classes.129. An **electronic** gambling system including a computerthat matches gamblers with plural gambling providers based at leastin part through classifying the gambling providers using **rights**management information.130. An **electronic** gambling system as in claim 129 whereinthe computer includes means for classifying the gamblers based atleast in part on **rights** management information.131. An **electronic** gambling system as in claim 129 whereinthe computer includes at least one protected processing environment.

1 132. An **electronic** gambling system as in claim 129 wherein the computer uses at least one control set to classify, select and/ormatch at least one of said gambling providers, and/or gamblers.133. An **electronic** ticketing system including a computerthat matches recipients with tickets to events through classifying saidrecipients, said system including a computer that matches ticketsand/or said events based at least in part on **rights** managementinformation.134. An **electronic** ticketing system as in claim 133 whereina recipient provides a request containing event and **rights**management criteria, and the computer matches the recipient with aprovider based at least in part on said classifying process.135. An **electronic** ticketing system as in claim 133 whereinthe **rights** management information includes method of paymentinformation.

Country	Number	Kind	Date

Claims:

...characteristic of said participant and/or participant installation.
365AMENDED SHEET (ARTICLE 19)means for associating plural digital credentials corresponding to saidcharacteristics with certain **digital** information and/or **electronic** events for usagegovernance;means for requesting at least one form of **digital** processing of said **digital**information;means for testing for the presence of said first and second **digital**credential. andmeans for responding to said request based at least in part on said test, wherein said responding to said request is governed at... ...for enabling peersto perform certificate authority functions, said system including plural commerce node end-users having associated end-user installations, and at least one **digital**information rightsholder, said system comprising:at least one securely interoperable commerce node at a site of a firstcommerce node end user;means for enabling said first end user to issue certificates to others of saidcommerce node end-users and/or end-user installations. andmeans for enabling said **digital** information rightsholder and/or said first end user to at least in part manage usage **rights** related to certain dialtal information as a result of said rightsholder and/or said first end-user associating one or more said end-user issued certificates with certain processing of said **digital** information.165. A distributed trust platform comprising:means for securely establishing a unique site identifier;366AMENDED SHEET (ARTICLE 1 9)a secure installation arrangement for securely installing end-user **electronic** commerce installations and for securely managing software installation and/orsoftware updating;means for securely associating rules and controls with certain **digital**information;means for securely distributing said **digital** information for use at said enduser **electronic** commerce installations; andmeans for controlling use of at least a portion of said **digital** information in response to said associated rules and controls.166. An arrangement for reporting **electronic** commerce event, userprofiling, and surveying information in the context of a system including distributed **electronic** commerce nodes including means for monitoring usage of **digital** information and means for securely reporting at least a part of informatiollrelated to said monitored usage from said commerce nodes to at least one... ...an arrangement that electronically instructs said system service. inaccordance with rules and controls associated with said reported usage related information, to electronically report to **digital** information rightsholders.167, Distributed **electronic** system apparatus for supporting distributedmicro-transaction auditing and processing, said apparatus comprising:protected, distributed commerce nodes for auditing usage of **digital**information, plural of said commerce nodes including means for managing micropayment related activity related to said usage of **digital** information based. at leastin part. on control information provided by a first party; and367AMENDED SHEET (ARTICLE 1 9)at least one commerce... ...168. In a system including peer-to-peer

commercial participant securecommerce nodes for permitting plural parties to participate in a distributed commercial process via **electronic** instructions, apparatus for transaction authority management of distributed commercial activities, said apparatus comprising:a transaction authority for assisting in the governance ofa distributedcommercial process... ...commercial participant secure commerce nodesfor at least in part enforcing said governance.169. In a communications network for communicating at least in partsecured **digital** information provided by a first commercial party to a second commercial party different from said first commercial partN a distributed**electronic** security checkpoint system comprising:at least one checkpoint **electronic** switch for at least in part receiving said secured **digital** information, and for interacting with at least a portion of said received secured information. including means for acquiring information re ated to said secured information... ...least one of certifyinizr. authenticating, validating, and/or otherwise asserting and/or testing saidinformation so as to provide a trusted commerce service, said checkpoint**electronic** switch including a communications arrangement for furthercommunicating at least a portion of said secured **digital** information to said second commercial party different from said first commercial party.368AMENDED SHEET (ARTICLE 19). A **digital** broadcasting network, said apparatus comprising:means for securely providing **digital** information to plural participants in a cooperative arrangement of network information hosting and/or other serviceparties;means for basing variables related to said provision of said **digital**information at least in part upon the specific attributes of each said party and/orclasses to which said parties belong;means for commercially redistributing at least a portion ofsaid **digital**information from at least certain of said parties to further parties, andmeans for representing said cooperative arrangement to directly and/orelectronically negotiate compensation arrangements related to said provision of **digital** information.171. A secure messaging system comprising:means for packaging **digital** information. at least in part secureh in an**electronic** container for transmission by a first party;means for employing a directory service to provide **electronic** addressinformation to direct said container to at least one additional party:means for transmitting said container to said at least one additional party,means for providing authentication for at least a part of said **digital**information and/or for said container; andmeans for preventing said first party from effectively denving that saidfirst party sent at least a portion of said **digital** information and/or said container to said at least one additional party.172. In a distributed **electronic** commerce system including pluralprotected end-user participant commerce nodes distributed for use by end-user participants in commercial processes, said end-user participant commerce nodes369AMENDED SHEET (ARTICLE 19)receiving at least in part protected **digital** information, a **rights** repository arrangement disposed remotely from said end-user participants, said **rights** repository enabling said end-user participant node to securely, separately receive **rights** permission information from said remote **rights** repository to. at least in part, enable a desired usage of at least a portion of said **digital** information at said end-user participant commerce node.173. A mixed commerce infrastructure comprising:plural, distributed commerce utility systerns providing trusted commerceservices:plural, distributed, trusted commerce appliances supporting end-user**electronic** commerce activity; andat least one communications arrangement for securely conveying dipritalinformation between said end-user **electronic** commerce appliances and at least one said commerce utility system, securely conveying **digital**

information between two or more of said commerce utility systems, and securely conveying **digital** information between said two or more of end-user commerce appliances.174. A hierarchical commerce infrastructure comprising:plural trusted, distributed commerce appliances having associated users:means for establishing a programmed hierarchical **rights** managementrelationship between said plural distributed commerce appliances and/or said usersof said distributed commerce appliances; andmeans for separately producing, at least in part in combination with at least a portion of said programmed hierarchical **rights** relationship and at least in part by the action of a more hierarchically senior: (a) distributed commerce appliance. (b) user using a distributed commerce appliance...least one of said end-user commerce nodes.176. A virtual computer comprising:a trusted commerce utility system for at least in part managing use**rights** related to resources available at plural distributed commerce nodes,means for establishing use **rights** information to at least in part governuse of physical and/or logical resources available for use at, at least one of'. saiddistributed commerce nodes;means for securely communicating at least a portion of said use **rights**information to said at least one remote distributed commerce node, andmeans for employing resources at said at least one said distributedcommerce nodes for use in said virtual computing arrangement based. at least inpart, on said use **rights** information177. A virtual, networked banking system comprising:371AMENDED SHEET (ARITICLE 19)a **web** of plural. separately managed banking protected processingenvironments; anda communications arrangement that communicates control informationsecurely between said plural, separately managed banking protected processingenvironments;wherein said **web** of plural, separately managed protected processingenvironments includes a governing arrangement that governs one or more banking activities, by at least in part managing, at least in part through use of rules and controls. interacting **electronic** processes at least in part operating under the control ofsaid plural banking protected processing environments. said processes beina, related to one or more of.- (1) the **electronic** storage of currency, (2) the **right** to lend money to at least one participant, (3) the fulfillment of payment obligations, (4) the management of **electronic** bills and/or other obligations, and (5) the ability to deliver or otherwise communicate one or more currencv objects. 178. A system for supporting payment settlement related. at least in part. to electronically **rights** managed **electronic** commerce. said system including plural distributed **electronic** commerce nodes located at remote end-user sites. saidsystem comprising:at least one financial clearinghouse including:a communications arrangement for securely receiving paymentrelated information from at least one of said distributed **electronic**commerce nodes; anda protected processing environment coupled to the communicationsarrangement, the protected processing environment processing at least aportion of said payment related information, said processing including atleast in part governing payment fulfillment information at least in partbased upon **electronic rights** management control information processed.372AMENDED SHEET (ARITICLE 1 9)wherein the communications arrangement securely communicates paymentfulfillment related information to at least one of employs a protected processing environment to access said payment fulfillment related information. 179. A fulfillment server for efficiently managing **electronic** requests. saidfulfillment server comprising:a communications arrangement for securely receiving **electronic** requestinformation from at least one distributed, trusted **electronic** commerce node and for securely receiving,

from a remote location, rule based control information securelv associated with said **electronic** request information, said rule based control information operating with fulfillment server control information to format least one control set arrangement; anda processing arrangement... ...and (c) seeking further information related to said request.wherein said processing arrangement securely responds, through saidcommunications arrangement, to said one of said distributed **electronic** commerce nodes to provide feedback regarding said request information.180. A system for supporting delegated **electronic rights** comprising:373AMENDED SHEET (ARTICLE 19)plural distributed trusted **electronic** commerce nodes for use by pluralseparate parties; anda **digital** credentialing arrangement that associates a **digital** credential with one or more of said parties and/or nodes, wherein said credential. in combination with protected control information, enables the **right** to said one or more parties and/or nodes to electronically represent and/or exercise **rights** possessed by one or more other parties and/or nodes and enables at least one **right** to represent and/or exercise at least in part through the use of **electronic** control information,wherein at least one of said trusted **electronic** commerce nodes governssaid **right** to represent and/or exercise by processing at least a portion of saidcontrol information,181. A system for supporting a virtual entity comprising:plural distributed, trusted **electronic** commerce nodes for use by pluralparties, one or more said trusted **electronic** commerce nodes securely creating one or more **digital** credentials representing a virtual entity comprising a cooperative participation among plural parties and/or nodes for one or more commercialpurposes,a **digital** credentialing arrangement that issues **digital** credentials to said plural parties and/or nodes to at least in part represent the identity of said partiesand/or nodes; anda secure communications arrangement that securely communicates amongsaid plural parties and/or nodes, **digital** information related to at least in part theidentity of said parties and/or nodes,wherein said system employs at least one of said one... ...entity to at least in part participate in at least one commercial process.374AMENDED SHEET (ARTICLE 1 9). A system for securely electronically delivering **digital** informationbetween plural participants employ'rigprotected **electronic** environments, saidsystem comprising:a secure communications arrangement for securely communicatingselected **digital** information between two or more participant parties supported by at least one trusted service provider participant, wherein said trusted provider supports archiving and/or authenticating of transaction related information; means at two or more of said trusted **electronic** environments for securely generating secure control infori-nation and for securely governing at least a portion of said communicating and use of said selected, communicated **digital** information through use of said generated control information. means coupled to each of said trusted **electronic** environments for storing information related to communication and/or usage of said communicated **digital**information at each participant site; andmeans at said trusted service provider participant for performing trusted archival and/or authentication services related to said selected dicital information1 83. An arrangement for reporting **electronic** commerce event. userprofiling, and surveying information in the context of a system includingdistributed **electronic** commerce nodes having means for monitoring andgoverning usage of **digital** information, and means for collecting user profiling and/or survey information and securely reporting information related to said user profiling and/or surveying from at... ...service, inaccordance with rules and controls associated

with said communicated profile and/or survev related information, to electronically, securely communicate to at least one **digital** information rightsholder, certain of said user profiling and survevin information related to usage.9375AMENDED SHEET (ARTICLE I 9). A trusted third party certification authority arrangement for use withthree or more **electronic** commerce participant sites each having at least one associated user, said trusted third party certification authority arrangementcomprising:a certifying arrangement for certifying at least one commercialcapability, commitment, and/or other attribute related to at least two of said three or more **electronic** commerce participant sites and/or said users of said sites, and securely providing an associated **digital** credential to at least one **electronic** commerce participant site different from said at least two of said three or more **electronic** commerce participant sites and/or said users of said sites.wherein said at least one different **electronic** commerce participant siteemploys said **digital** credential in the performance of a commercial activity.185. A trusted arrangement including trusted installations for couplingtrusted and untrusted activities at plural end user...component are concealed from the users of the trusted arrangement.186. An infrastructure for multi-nodal commercial processing comprising:376AME14DED SHEET (ARTICLE 19)secure **electronic** commerce node arrangements at independent participantsites for securely processing programmed **rights** arrangements for. at least in part.securely managing multi-steps of a commercial process; andat least one communication arrangement for securely communicating atleast a portion of said **rights** control information between a first of said commerce node arrangements and a second of said commerce node arrangements to provide control information to said second... ...or participant B isthe same as participant D. 188. An arrangement as in claim 163 wherein at least one of said first and second **digital** credentials comprises a **digital** certificate. 189. An infrastructure as in claim 1 74 wherein said distributed commerce appliances comprise a distributed commerce utility system.190. Apparatus as in claim... ...19). Apparatus as in any one of the preceding claims 156-190 furtherincluding means for performing a negotiation process that supports bidding, auctions or **electronic** contracts.192. Apparatus as in any one of the preceding claims 156-191 furtherincluding means for supporting a secure multiparty negotiation process.193. Apparatus... ...claims 156-194 furtherincluding means for allowing a value chain participant to stipulate at least one aspect of information privacy control.196. In an **electronic** clearing arrangement including plural. distributedclearinghouse nodes performing **digital** information usage audit functions and maintaining at least one database containing a local store of information related to multiple uses of **digital** information, said database including rules securelysupplied by at least one **digital** information rightsholder, and a centralclearinghouse facility remote from at least some of said plural. distributedclearinghouse nodes, said central clearinghouse facility including:a communications infori-nation representative of said multiple378AMENDED SHEET (ARTICLE 19)uses of **digital** information from plural distributed c
learinghouse nodes'said at
least one databases, and securely supplying to said remote clearinghouse nodes, separately from said rules supplied by said **digital** information rightsholder, rules for securely managing at least one portion and/or other aspect of use of said multiple **digital** information by said plural, distributed clearinghouse nodes, wherein said plural, distributed clearinghouse nodes securely manage said at least one portion and/or other

aspect of... ...portion of said local store of information and said rules securely and separateiv supplied by said clearinghouse facility and said at least one third party **digital** information rightsholder.197. In a cooperative, distributed **rights** management commercial systemincluding at least one value chain participant node, said system providing plural system services for use by **digital** information rightsholders, a commerce service center capable of communicating with said value chain participant mode for securely supporting **electronic** commerce by at least in part providing said plural system services comprising two or more of (1) financial clearing, (2) usage information clearing, (3) **rights** and permissions clearing, (4) certificate authoritV services, (5) directory services, (6) advertising management services. (7) repository, archiving, back up, and/or non-repudiation services, (8) certifving services validating that **digital** information and/or events have satisfied applicable commerce rules and controls. (9) managing distributed transaction processing in accordance with applicable commerce rules and controls. and (IO) user and/or class profiling and/or marketing analysis including tailoring the direction of **digital** information to one or more specific parties and/or class of parties based at least in part upon said profiling and/or other analysis. said... ...center to enabling secure, cooperative use of said system services.379AMENDED SHEET (ARTICLE 1 9). In a distributed commerce system supporting end-users using **digital**information, a service operation that performs **electronic** commerce support services, said service operation receiving **digital** information reflecting said enduser use of said **digital** information, said service operation including a secure communications arrangement for communicating **digital** information reflecting end-user use of said **digital** information with at least one additional service operation.199. In a rules managed **electronic** commerce system for directing themovement of **digital** information among participants having established identities,a commerce service center comprising:a communications arrangement for receiving acquired user profile and/orpreference information associated with said participants; anda directing arrangement for directing other **digital** information to at least one of said participants based at least in part upon said conveyed profile and/or preference information, said directed **digital** information at least in part ensuring satisfaction of requirements specified by rightsholders in said directed **digital** information through use, at least in part. of rules and controls specified by saidrightsholders200. In a rules and controls based, distributed commerce svstem...plural participants comprising a combination of plural. separate authorized commerce service providers and plural authorizedend-users; and380AMENDED SHEET (ARTICLE 1 9)transferring **digital** information securely between one or more end-usersites and plural, separate commerce service providers in response, at least in part, to commerce rules and controls established by one or more of said participants.201. Inasystemforreportingelectroniccommerceevents.userprofiling,and surveying information, said system including distributed **electronic** commerce nodes that securely monitoring usage of **digital** information and securely report information related to said monitored usage from said commerce nodes to at least one commerce utility system service, at least one... ...service, said commerce utility system service including an arrangement that electronically controls, in accordance xvith rules and controls associated with said reported usage related information, **electronic** reporting to **digital** information rightsholders of'certain of said information related to usage, and reports differing usage information to different rightsholders as required by rules and controls, and wherein said

usage information includes at least some information not provided in useable form to said commerce utility system service. 202. In a distributed **electronic** system for supporting distributed microtransaction auditing and processing, said system including protected. distributed commerce nodes for auditing usage of **digital** information, at least some of said commerce nodes including means for managing micro-payment related activity related to said usage of **digital** information based, at least in part. on control information provided by a first party, said system further characterized by at least one commerce utility system... ...based, at least in part, on control information provided by a second party different from said first party.381AMENDED SHEET (ARTICLE 1 9). An **electronic** commerce and/or **rights** management system forperforming at least one clearing operation, the system comprising:a first **electronic** appliance (I 00),a second **electronic** appliance (I 00'), andan **electronic** communications network (I 50) that allows the first andsecond **electronic** appliances (100, 100') to exchange **digital** signals,characterized in that:the first **electronic** appliance (I 00) performs at least a first part of theclearing operation, andthe second **electronic** appliance (I 00') performs at least a second part of the clearing operation.204. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first part of the clearing operation includes at least one micropayment aggregation task, and the second part of the clearing operation includes at least one payment settlement task.205. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that that the first **electronic** appliance (I 00) comprises a consumer appliance, and the second **electronic** appliance (I 00') is installed, at least in part, within a clearing institution.206. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that at least the first **electronic** appliance (I 00) includes a protected processing environment (1 54).207. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first part of the clearing operation382AMENDED SHEET (ARTiCLE 19)comprises a usage metering task (I 16).208. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first part of the clearing operation comprises at least one task conditioned on a **digital** certificate (504).209. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first part of the clearing operation comprises at least one **rights** management task.2 1 0. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first part of the clearing operation comprises at least one **electronic** currency management task.21 1. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that most of the clearing operation is performed by the first appliance (I 00).212. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that most of the clearing operation is performed by the second appliance (100').213. An **electronic** commerce and/or **rights** management system, as inclaim 203 further characterized in that the system further includes a third **electronic** appliance (I 00") coupled to at least one of the first and second **electronic** appf iances (I 00, I 00') through the network (I 50), the third **electronic** appliance performing a third part of the clearing operation.214. An **electronic** commerce and/or **rights** management system as in383AMENDED SHEET (ARTICLE 19)claim 203 further characterized in that each of the first and second appliances (I 00, I 00') are capable of performing any of a financial clearing operation, a usage clearing operation, a **rights** and

permissions clearing operation, a certifying authority operation, a transaction authority operation, and a secure directory services operation, and each of said operations may be distributed in different ways between the first and second appliances (I 00, I 00').215. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the **electronic** network (I 50) couples the first and second **electronic** appliances (I 00, I 00') to a commerce utility system **web**.216. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that an **electronic rights** holder canelectronically choose between the first **electronic** appliance (100) and the second **electronic** appliance (100').217. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first and second **electronic** appliances (I 00, I 00') work together to perform overall transaction clearing.218. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that each of the first and second appliances (100, 100') performs each of. at least one financial clearing operation, at least one usage clearing operation, at least one **rights** and permissions clearing operation, at least one certifying authority operation, at least one transaction authority operation, and at least one secure directory services operation.219. An **electronic** commerce and/or **rights** management system as in384AMENDED S14EET (ARTICLE 19)claim 203 further characterized in that the first **electronic** appliance (I 00) comprises a hierarchy of plural commerce utility systems (90(l),... 90(n)).220. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first **electronic** appliance (I 00) is organization-specific.22 1. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first **electronic** appliance (I 00) is vertically specialized.222. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first **electronic** appliance (I 00) is specialized by territory and/or jurisdiction.223. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that the first and second **electronic** appliances (I 00. I 00') communicate and coordinate as peers and in a hierarchy.224. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that that clearing operation includes processingpayment related information, and performing at least one payment relatedtransaction.225. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that that clearing operation includes processing usage related information and performing at least one usage reporting action.226. An **electronic** commerce and/or **rights** management system as in385AMENDED SHEET (ARTICLE 19)claim 203 further characterized in that that clearing operation includes receiving at least one request, and performing at least one associated **rights** management transaction.227. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that that clearing operation includes issuing at least one **digital** certificate.228. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that that clearing operation includes securely providing directory information.229. An **electronic** commerce and/or **rights** management system as inclaim 203 further characterized in that that clearing operation includes performing at least one process management transaction.230. An **electronic** commerce and/or **rights** management system as inclaim 203 whether the first and second parts of the clearing operation support one another.23 1. An **electronic** commerce and/or **rights** management

system as inclaim 203 wherein at least one of the first and second **electronic** appliances (I 00, 100') includes a **rights** operating system that supports a collection of service application components defining at least one service function.232. A method for supporting a commercial **electronic** commerceinfrastructure enabling plural networked commercial arrangements. said method comprising the steps of386AMENDED SHEET (ARTICLE 1 9)a. Providing security, communication, and certification information formaintaining an interoperable framework for distributed, trusted,programmable **electronic** commerceb. Supporting, within said framework, **rights** components and/or other**rights** language for operation within protected **electronic** commerceinstallations separately operated by **electronic** commerce participantsc. Participating, by plural such participants, in programmed commercialwebs, plural of said webs involving differing combinations of saidseparately managed protected processing environmentsd. Governing, at least in part; the operation of said commercial websthrough the enforcement of control information within said protected**electronic** commerce instaRations, wherein such control informationprocessed within at least one of said protected **electronic** commerceinstallations was specified by at least two of said **web**'s participants233. A method for securely governing a multi-nodal commercial process,said method comprisinga. Operating distributed, secure **electronic** commerce nodes atindependent participant sitesb. Programming plural, differing commercial **rights** arrangements forprocessing within plural of said secure **electronic** commerce nodesc. Communicating securely said **rights** information to at least in partsecurely manage the operation of a multi-nodal multi-step processd. Managing at least in part securely a commercial process at least in partunder the control of said **rights** information operating within secure**electronic** commerce nodes, wherein at least one step securely occursat one independent site and another step securely occurs at a secondindependent site387AMENDED...

18/K/16 (Item 4 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT
(c) 2009 WIPO/Thomson. All rights reserved.

Country	Number	Kind	Date

Detailed Description:

...of
metering, auditing, billing, and budgeting methods,
the present invention is able to efficiexitly,
concurrently support multiple financial currencies
(e.g. dollars, marks, yen) and **content** related
budgets, and/or billing increments as well as verv
flexible content distribution models.

support, complete, modular separation of the control
structures related to (1) content event triggering, (2)
auditing, (3) budgeting (includiner specifying no **right**
t) C1
of use or unlimited **right** of use), (4) billing, and (5)
identity (VDE installation, cli
user 1 1 1 ient name,
department, network, and/or user, etc.). The
independence of... ...performing home banking, managing
advertising services, etc. VDE modular separation
of these basic capabilities supports the programming
of plural., "arbitrary" relationships between one or
differing **content** portions (and/or portion units) and
budgeting, auditing, and/or billing control
information. For example, under VDE, a budget
limit of $200 dollars or 300...trator's control information, which may take precedence
over an end-user's control information. A path of distribution
participant's ability to set such **electronic** content control
- 132 - COT
1111M UOT olaialM uodn pasuq uolquuuojuT
lo-quoO aAj4RU.Iajp
uaamlaq sasomp -io/pu-e) uoiquuLiojm
loiluoo Bui sTxa aouldai
.io does
not directly participate in the handling of **electronic** content
(and/or appliance) and/or control information for such content
(and/or appliance). Such control information may be provided in
secure form using VDE... ...secure subsystems, and a pathway of VDE content
control information participant's VDE 'installation secure
subsystem. This control information may relate to, for example,
the **right** to access credit supplied by a financial services
provider, the enforcement of regulations or laws enacted by a
gov@rnment agency, or the requirements of... ...or manner of reporting of usage
information received by such customer. Such control information
may, for example, enforce societal requirements such as laws
related to **electronic** commerce.

i34
VDE content control information may apply differently to
different pathway of content and/or control information handling
participants. Furthermore, permissions records **rights** may be
added, altered, and/or removed by a VDE participant if they are
allowed to take such action. **Rights** of VDE participants may be
defined in relation to specific parties and/or categories of parties
and/or other groups of parties in a chain... ...or parties. may be limited i the number of

in
modifications. and/or degree of modification, they may make.

At least one secure subsystem 'in **electronic** appliances of
creators, distributors, auditors, clearinghouses,. client
administrators, and end-users (understandina that two or more
r-11
of the above classifications may describe a... ...information;
2. Storing control and metering related information;
3. Managing communications;
- 135
. Processing core control programs, along with
associated data, that constitute control information
for **electronic** content and/or appliance **rights**
protection, including the enforcing of preferences
and requirements of VDE participants.

Normally, most usage, audit, reporting, payment, and
distribution control methods are themselves at least... ...e.g. encrypted and
authenticated) communications when passing information
between the participant location (nodes) secure subsystems of a
VDE arrangement, important components of a VDE **electronic**
agreement can be reliably enforced with sufficient security
(sufficiently trusted) for the intended commercial purposes. A
VDE **electronic** agreement for a value chain can be composed, at
least in part, of one or more subagreements between one or more
subsets of the value chain participants. These subagreements
are comprised of one or more **electronic** contract 'compliance"
elements (methods including associated parameter data) that
ensure the protection of the **rights** of VDE participants.

- 136
The degree of trustedness of a VDE arrangement will be
primarily based on whether hardware SPUs are employed at
participant location... ...enforced (within the security limitations of a given VDE security
implementation design). This control information can determine,
for example.

(1) How and/or to whom **electronic** content can be
ided, for example, how an electro
provi iuc property
can be distributed;
(2) How one or more objects and/or properties, or...negotiation establishes what
control information shall constitute the resulting
control information set for a given piece of VDE
managed content and/or VDE installation.

139

Electronic Agreements and **Rights** Protection

An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and **rights** protection for, **electronic** agreements implemented through the use of the present invention. Such agreements may involve one or more of

(1) creators, publishers, and other distributors, of **electronic** information,

(2) financial service (e.g. credit) providers,

(3) users of (other than financial senrice providers) information arising from content usage such as content specific... ...marketing, and government agencies,

(4) end users of content,

(5) infrastructure service and device providers such as telecommunication companies and hardware

- 140

manufacturers (semiconductor and **electronic** appliance and/or other computer system manufacturers) who receive compensation based upon the use of their services and/or devices, and

(6) certain parties described by **electronic** information.

VDE supports commercially secure 'extended" value chain **electronic** agreements. VDE can be configured to support the various underlying agreements between parties that comprise this extended agreement. These agreements can define important **electronic** commerce considerations including.

(1) security,

(2) content use control, including **electronic** distribution,

(3) privacy (regarding, for example, information concerning parties described by medical, credit, tax, personal, and/or of other forms of confidential information),

(4) management of financial processes, and

- 141

(5) pathways of handling for **electronic** content, content and/or appliance control information, **electronic** content and/or appliance usage information and payment and/or credit.

VDE agreements may defirie the **electronic** commerce relationship of two or more parties of a value chain, but such

agreements may, at times, not directly obligate or otherwise directly involve other VDE value chain participants. For example, an **electronic** agreement between a content creator and a distributor may establish both the price to the distributor for a creator's content (such as for a... ...end-user agrees to certain requirements for using the distributed product such as accepting distributor charges for content use and agreeing to observe the copyright **rights** of the creator. A third agreement might exist between the distributor and a financial clearinghouse that allows the distributor to employ the clearinghouse's credit agreement can establish the **rights** of all parties to **content** usage information, including, for example, the nature of information to be received by each party and the pathway of handling of content usage information and... ...In the above example, these six agreements could comprise agreements of an extended agreement for this commercial value chain instance.

VDE agreements support evolving ('living") **electronic** agreement arrangements that can be modified by current and/or new participants through very simple to sophisticated "negotiations' between newly proposed content control information interacting...paplAoid aju saidoo T4:)ns sr 2uol os liao@xunb mpualu3 i9d CVZSIIL6Sfl/13d 6OZ60/86 OM

(c) secure financial transaction capabilities related to both **electronic** information and/or appliance usage and other **electronic** credit and/or currency usage and administration capabilities,

(d) privacy protection for usage information a user does not wish to release, and

(e) "living" **electronic** information content dissemination models that fle)dbly accommodate.

(1) a breadth of participants,

(2) one or more pathways (chains) for: the handling of content, content and/or appliance control information, reporting of content and/or appliance usage related information, and/or payment,

(3) supporting an evolution of **terms** and conditions incorporated into content control information, including use of **electronic** negotiation capabilities,

. 146

content to form new content aggregations, and

(5) multiple concurrent models.

Secure Processing Units

An important part of VDE provided by the... ...invention is the core secure transaction control arrangement,
herein called an SPU (or SPUs), that typically must be present in each user's computer, other **electronic** appliance, or network.

SPUs provide a trusted environment for generating decryption keys, encrypting and decrypt' g information, managing the
t3 in
secure communication of keys and other information between **electronic** appliances (i.e. between VDE 'installations and/or between plural VDE 'instances within a single VDE installation), securely accumulating and managing audit trail, reporting, and... ...of certain control software, one or more tamper resistant hardware modules such as a semiconductor or semiconductor chipset (including, for example, a tamper resistant hardware **electronic** appliance peripheral device), for use within, and/or operatively connected to, an **electronic** appliance. With the present invention, the trustedness of a hardware SPU can be enhanced by enclosing some or all of its hardware elements within tamper...IvME processes.

A VDE node's hardware SPU is a core component of a VDE secure subsystem and may employ some or all of an **electronic** appliance's primary control logic, such as a rMicrocontroller, microcomputer or other CPU arrangement. This primary control logic may be otherwise employed for non VDE purposes such as the control of some or all of an **electronic** appliance's non-VDE functions. When operating in a hardware SPU mode, said primary control logic must be sufficiently secure so as to protect
- 148
and conceal important VDE processes. For example, a hardware SPU may employ a host **electronic** appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute
-with a certain degree of security... ...5B show an example of an 'object";
FIGURE 6 shows an example of a Secure Processing Unit ("SPU');
FIGURE 7 shows an example of an **electronic** appliance;
FIGURE 8 is a more detailed block diagram of an example of the **electronic** appliance shown in FIGURE 7;
FIGURE 9 is ...and control processing unit;
Figure 9B shows an example secure processing unit integrated with a standard CPU;
151
FIGURE 10 shows an example of a "**Rights** Operating

FIGURE 70 shows an example of multiple VDE **electronic** appliances connected together with a network or other c o mmuMnlications means;

Figure 70A shows how content may be prepared for printing and encrypted inside a PPE, then decrypted inside a printer;

Figure 70B shows how characters may be selected from slightly different fonts in order to place an **electronic** fingerprint or water-mark into printed output;

- 161

Figure 70C shows how characters in a font may be permuted to render a printed page unusable without the corresponding scrambled font;

FIGURE 71 shows an example of a portable VDE **electronic** appliance;

FIGURES 72A-72D show examples of 'pop-up' displays that may be generated by the user notification and exception interface;

FIGURE 73 shows an... ...a 'smart object";

FIGURE 7 4 shows an example of a process using "smart objects";

FIGURES 75A-75D show examples of data structures used for **electronic** negotiation;

FIGURES 75E-75F show example structures relating to an **electronic** agreement;

FIGURES 76A-76B show examples of **electronic** negotiation processes;

- 162

FIGURE 77 shows a further example of a chain of handling and control;

FIGURE 78 shows an example of a VDE "repository may be part of an "**electronic** hiLThwa 'that carries **electronic** information from place to place. Lines 202 connect information utility 200 to other people such as for example a consumer 208, an office 210, a... ...with delivering information about a transaction, or it may be one of the transaction participants.

For example, the video production studio 204 in the upper **right**-hand comer of Figure 1 may create video/television programs. Video production studio 204 may send these programs over lines 202, or may use other video production studio or information utility 200 has arranged for these consumers to have appropriate 'rules and controls" (control information) that give the consumers **rights** to use the programs.

Even if a consumer has a copy of a video program, she
cannot watch or copy the program unless she has... ...house 214 may act as a distributor
for an author 206. The
publishing house 214 may distribute rigr1its to use "content" (such
as computer software, **electronic** newspapers, the video produced
by publishing house 214, **audio**, or any other data) to consumers
such as office 210. The use **rights** may be defined by "rules and
controls' distributed by publishing house 216. Publishing house
216 may distribute these "rules and controls' %vith the content,
but this is not necessary. Because the **content** can be **used** only
by consumers that have the appropriate 'rules -and controls,'
content and its associated "rules and controls' may be
distributed at different times, in different... ...participants. The ability of VDE to securely
distribute and
- 168
enforce 'rules and controls' separately from the content they
apply to provides great advantages.

Use **rights** distributed by publishing house 214 may, for
example, permit office 210 to make and distribute copies of the
content to its employees. Office 210 may...office, or
it may permit only specified employees and/or groups to access
certain information.

Figure 1 also shows an information delivery service 216
delivering **electronic** storage media such as 'CD ROM" disks to
consumers 206. Even though the **electronic** storagempdia
themselves are not delivered electronically by information utility
200 over lines 202, they are still part of the virtual distribution
environment 100. The **electronic** storage media may be **used** to
distribute **content**, "rules and controls,' or other information.

169
Example of What's Inside Information Utility 200
"Information utility" 200 in Figure 1 can be a collection... ...utility participants 200a-200g
could
each be an independent organization/business. There can be any
number of each of participants 200a-200g. In this example,
electronic 'switch' 200a connects internal parts of information
utility 200 to each other and to outside participants, and may
also connect outside participants to one another.

Information utility 200 may include a 'transaction
processor" 200b that processes transactions (to transfer
electronic funds, for example) based on requests from
participants and/or report receiver 200e. It may also include a

"usage analyst" 200c that analyzes reported usage... ...102 may also specify
"rules and controls" for distributinLr the content. These
distribution-related "rules and controls' can specify who has
permission to distnibute the **rights** to ...Arrow 104 shows the content creator 102 sending the
'rules and controls" associated with the content to a VDE rizhts
distributor 106 Nistributor') over an **electronic** hiLrhwa 108 (or
by some other path such as an optical disk sent by a delivery
service such as U. S. mail). The content can be distributed over
the same or different path **used** to send the "rules and controls.'
The distributor 106 generates her own "rules and controls" that
relate to usage of the content. The usage-related... ...usage-related "rules and controls'
must be consistent with the
'rules and controls" specified by content creator 102.

Arrow 110 shows the distributor 106 distributing **rights** to
use the content by sending the content's 'rules and controls" to a
conten use 112 such as a consumer. The content user 112...content creator 102.

Every VDE participant in "chain of handling and control"
is normally subject to "rules and controls." "Rules and controls"
define the respective **rights** and obligations of each of the various
- 174
VDE participants. "Rules and controls" provide information and
mechanisms that may establish interdependencies and
relationships between the... ...mark up" the wholesale pnice of goods. Figure 2A
shows an example in which certain "rules and controls" persist
unchanged from content creator 102 to **content** user 112; other
"rules and controls' are modified or deleted by distributor 106;
and still other "rules and controls" are added bv the distributor.

"Rules...appropriate permission, if
required. This ability to securely control what information is
revealed and what VDE participant(s) it is revealed to allows the
privacy **rights** of 0 VDE participants to be protected.

- 176
Rules and Contents' Can Be Separately Delivered
As mentioned above, virtual distribution environment 100
"associates" content with corresponding "rules and controls," and
prevents the **content** from being **used** or accessed unless a set of
corresponding 'rules and controls' is available. The distributor
106 doesn't need to deliver **content** to control the content's
distribution. The preferred embodiment can securely protect
content by protecting corresponding, usage enabling "rules and
controls" against unauthorized distribution and... ...content that has already

been (or will in the future be) delivered. "Rules and controls" may be delivered over a path different from the one **used** for **content** delivery. "Rules and controls" may also be delivered at some other time. The content creator 102 might deliver content to content user 112 over the **electronic** highway 108, or could make the content available to anyone on the highway. **Content** may be **used** at the time it is delivered, or it may be stored for later use or reuse.

- 177
The virtual distribution environment 100 also allows payment... ...to a certain limit) to pay for usage of any content. A "credit transaction" can take place at the user's site without requiring any '**online**" connection or further authorization. This invention can be used to help securely protect the virtual 'credit card' against unauthorized use.

Rules and Contents' Define Processes...lacks permission will not have her request satisfied (No
- 178
Go'). As another example, each user request to turn to a new page of an **electronic book** may be satisfied ("Go'), but it may not be necessary to meter, bill or budget those requests. A user who has purchased a copy of... ...can be charged to the user), and treat all later requests to open the same novel as 'insignificant events." Other content (for example, searching an **electronic** telephone directory) may require the user to pay a fee for each access.

"Meter" process 404 keeps track of events, and may report usage to... ...so the information can't be accessed except as provided by its "rules and controls."
- 180 Normally, the container 302 is electroni rather than physical.

Electronic container 302 in one example comprises '**digital**" information having a well defmed structure. Container 302 and its contents can be called an 'object 300."
The Figure 5A example shows items 'within' and...a certain time.

Even then, the container 302 "contamis" the live feed (by reference) in this example.

Container 302 may contain information content 04 in **electronic** (such as "**digital**") form. Information content 304 could be the text of a novel, a picture, sound such as a musical performance or a reading, a **movie** or other video, computer

software, or just about any other kind of **electronic** information
you can think of. Other types of "objects' 300 (such as
- 181
'administrative obiects") may contain "administrattve" or other
I
information instead of or... ...s contents, who can distnibute the object,
and what other control mechanisms must be active. For
example, permissions record 808 may specify a user's **rights** to
use, distribute and/or administer the container 302 and its
content. Permissions record 808 may also specify requirements
to be applied by the budgets... ...on usage of information content 304, and how usage will be paid
for. Budgets 308 can specify, for example, how much of the total
information **content** 304 can be used and/or copied. The methods
310 may prevent use of more than the amount specified by a
specific budget.

"Other methods... ...descrambled, and
other processes associated with hancHing and controlling
information content 304. For example, methods 1000 may record
the ident1tv of anyone who opens the **electronic** container 302,
and can also control how information content is to be charged
based on "metering." Methods 1000 may apply to one or several
different... ...containers
302, as well as to all or specific portions of information content
304.

Secure Processing Unit (SPU)
The'*VDE participants" may each have an "**electronic**
appliaric ." The appliance may be or contain a computer. The
appliances may communicate over the **electronic** highway 108.

Figure 6 shows a secure processing unit ("SPU") 500 portion of
- 183
participant. SPU 500 processes information in a secure
environment 503, and stores important information
securely. SPU 500 may be emulated by software operating in a
host **electronic** appliance.

SPU 500 is enclosed within and protected by a "tampe
...in this example is an integrated circuit ("IC')
"chip" 504 including "hardwarg" 506 and 'fin-nware" 508. SPU
500 connects to the rest of the **electronic** apphance through an
"appliance link" 510. SPU'firmware" 508 in this example is
44 software" such as a "computer prograni(s)" "embedded' within
- 184 chip... ...Firmware 508 makes the hardware 506 work.

Hardware 506 preferably contains a processor to perform instructions specified by firmware 508. "Hardware" 506 also contains long-**term** and short-**term** memories to store information securely so it can't be tampered with. SPU 500 may also have a protected clock/calendar used for timing events. The SPU hardware 506 in this example may include special purpose **electronic** circuits that are specially designed to perform certain processes (such as "encryption" and 'decryption") rapidly and efficiently.

The particular context in which SPU 500 is... ...parts of processes shown in Figure 3. In some contexts, the functions of SPU 500 may be increased so the SPU can perform all the **electronic** appliance processing, and can be incorporated into a general purpose processor. In other contexts, SPU 500 may work alongside a general purpose processor, and therefore only needs to have enough processing capabilities to handle secure processes.

185
Figure 7 shows an example of an **electronic** apphance 600 including SPU 500. **Electronic** appliance 600 may be practically any kind of electrical or **electronic** device, such as.

a computer
a T.V. "set top' control box
a pager
a telephone
a a sound system
a video reproduction svstem
a video game player
a "smart" credit card
Electronic appliance 600 in this example may miclude a keyboard or keypad 612, a voice recognizer 613, and a display 614. A human user can input... ...and may view information on display 614.

Appliance 600 may communicate with the outside world through any of the connections/devices normally used within an **electronic** appliance. The connections/devices shown along the bottom of the drawing are examples.

'modem" 618 or other telecommunications link;
CD ROM disk 620 or other **rights**
operating system" 602 that manages appliance 600 and SPU 500 by controlling their hardware resources. The operating system

602 may also support at least one... ...602 provides a standardized, well defined, generalized 'interface" that could support and work with many different 'applications" 608.

Operating system 602 in this example provides '**rights** and auditing operating system functions" 604 and "other operating ,system functions" 606. The "**rights** and auditing operating
- 187
distribution environment 100. SPU 500 provides or supports many of the security functions of the '**rights** and auditing operating system functions' 402. The "other operating system functions" 606 handle general appliance functions. Overall operating system 602 may be designed from the beginning to include the "**rights** and auditing operating system functions' 604 plus the 'other operating system functions' 606, or the '**rights** and auditing operating system functions" may be an add-on to a preeidsting operating system providing the 'other operating system functions."
"**Rights** operating system" 602 in this example can work with many different types of appliances 600. For example, it can work with large mainframe computers, "minicomputers... ...also work 'in control boxes on the top of
television sets, small portable "pagers," desktop radios, stereo sound systems, telephones, telephone switches, or any other **electronic** appliance. This ability to work on big appliances as well as little appliances is called "scalable.' A "scalable' operating system 602 means that there can be a standardized interface across many different appliances performing a wide variety of tasks.

- 188 The "**rights** operating system functions" 604 are " services bascd' in this example. For example, "**rights** operating system functions" 604 handle summary requests from application 608 rather than requiring the application to always make more detailed "subrequests' or otherwise get involved with the underlying complexities involved in satisfying a sum ary request. For example, application 608 may simply ask to read specified information; "**rights** operating system functions" 604 can then decide whether the desired information is VDE protected content and, if it is, perform processes needed to make the information available. This feature is called "transparency." "Transparency" makes tasks easy for the application 608.

'**Rights** operating system functions' 604 can support applications 608 that "know" nothing about virtual distribution environment 100. Applications 608 that are 'aware" of virtual distribution

environment 100 mav be able to make more detailed use of virtual distribution environment 100.

In this example, "**rights** operating system functions" 604 are "event driven". Rather than repeatedly examining the state of **electronic** appliance 600 to deterr ='e whether a condition has arisen, the "**rights** operating system functions' 604 may respond directly to "events" or "happenings" within appliance 600.

- 189
In this example, some of the services performed by "**rights** operating system functions' 604 may be extended based on additional "components' delivered to operating system 602.

'**Rights** operating system finictions' 604 can collect together and use 'components' sent by different participants at different times. The "components' help to make the operating system... ...user'). Other components are designed to work with specific applications or classes of applications (e.g., some types of meters and some types of budgets).

Electronic Appliance 600
An **electronic** appliance 600 provided by the preferred embodiment may, for example, be any **electronic** apparatus that contains one or more microprocessors and/or microcontrollers and/or other devices which perform lo an&'or mathematical calculations. This may 'include computers; computer terminals; device controllers for use with computers; penipheral devices for use with computers; **digital** display devices; televisions; video and **audio**/video projection systems; channel selectors and/or decoders for use with broadcast and/or cable transmissions; remote control devices; video and/or **audio** recorders; media players including compact disc players, Videodisc players and
- 190
tape players; **audio** and/or video amphfiers; virtual reality machines; **electronic** game players- multimedia players; radios; telephones; videophones; facsimile machines; robots; numerically controlled machines including machine tools and the like; and other devices containing one or more microcomputers and/or microcontrollers and/or other CPU's, including those not yet in eidstence.

Figure 8 shows an example of an **electronic** appliance 600.

This example of **electronic** appliance 600 includes a system bus 653. In this example, one or more conventional general purpose

central processing units ("CPUs") 654 are connected to bus... ...for example, store information
on mass media such as a tape 670, a floppy disk, a removable memory card, etc. Communications controller 666 may allow **electronic** appliance 600 to communicate with other **electronic** appliances via network 672 or other telecommunications links.

Different **electronic** appliances 600 may interoperate ...comprise the same one or more non-secure secondary storage devices (such as a magnetic disk and a CD-ROM drive as one example) that **electronic** appliance 600 uses for general secondary storage functions. In some implementations, part or all of secondary storage 652 may comprise a secondary storage device(s... ...information.

Secondary storage 652 in this example stores code and data used by CPU 654 and/or SPU 500 to control the overall operation of **electronic** appliance 600. For example, Figure 8 shows that "**Rights** Operating System' CROS') 602 (including a portion 604 of ROS that provides VDE functions and a portion 606 that provides other OS functions) shown in... ...602 in particular may desirably be included in ROM 658 (e.g., "bootstrap' routines, POST routines, etc. for use in establishing an operating environment for **electronic** appliance 600 when power is applied).

Figure 8 shows that secondary storage 652 may also be used to store code ("application programs') providing user application...specifical-ly designed for VDE 100) can also access and take advantage of VDE functions 604.

SECURE PROCESSING UNIT 500
Each VDE node or other **electronic** appliance 600 in the preferred embodiment may include one or more SPUs 500. SPUs 500 may be used to perform all secure processing for VDE... ...data management processes including governing usage of, auditing of, and where appropriate, payment for VDE objects 300 (through the use of prepayments, credits, real-time **electronic** debits from bank accounts and/or VDE node currency token deposit accounts). SPU 500 may perform other transactions related to such VDE objects 300.

SPU...to complicate efforts to electrically determine the value of memory locations. These and other techniques may contribute to the security of barrier 502.

In some **electronic** appliances 600, SPU 500 may be

integrated together with the device microcontroller or equivalent
or with a device I/O or communications microcontroller into a... ...example, in one preferred
embodiment, SPU 500 may be integrated together with one or
more other CPU(s) (e.g., a CPU 654 of an **electronic** appliance) in
a single component or package. The other CPU(s) 654 may be
any centrally controlling logic arrangement, such as for example,
a microprocessor... ...integrated SPU/CPU
component is a standard feature of a widely distributed
microprocessor line. Merging an SPU 500 into a main CPU 654
of an **electronic** appliance 600 (or into another appliance or
appliance peripheral microcomputer or other microcontroller)
may substantially reduce the overhead cost of implementing
- 198
VDE 100. Integration...may also be integrated
into other peripheral devices, such as CD-ROM devices, set-top
cable devices, game devices, and a wide variety of other
electronic appliances that use, allow access to, perform
transactions related to, or consume, distn'buted information.

SPU 500 Tnternal Architecture
Figure 9 is a detailed diagram... ...be separate
packages within a secure SPU 500.

In the preferred embodiment, microprocessor 520 normally
handles the most security sensitive aspects of the operation of
electronic appliance 600. For example, microprocessor 520 may
manage VDE decrypting, encrypting, certain content and/or
appliance usage control information, keeping track of usage of
VDE secured content, and other VDE usage control related
functions.

Stored in each SPU 500 and/or **electronic** appliance
secondary memory 652 may be, for example, an instance of ROS
602 software, application programs 608, objects 300 containing
201
VDE controlled property content... ...VDE control information. ROS 602
includes software intended for execution by SPU microprocessor
520 for, in part, controlling usage of VDE related objects 300 by
electronic appliance 600. As will be explained, these SPU
programs include "load modules' for performing basic control
functions. These various programs and associated data are
executed...and/or replacement data and/or code. In the event of a
disabling and/or destruction of processes and/or information as
described above, the **electronic** appliance 600 may require a
secure VDE communication with an administrator,

clearinghouse, and/or distributor as appropriate in order to
reinitialize the RTC 528. Some... ...then.

It may be desirable to provide a mechanism for setting
and/or synchronizing RTC 528. In the preferred embodiment,
when communication occurs between VDE **electronic** appliance
- 204
and another VDE appliance, an output of RTC 528 may be
compared to a controlled RTC 528 output time under control of
the...otherwise be performed by software
operating on microprocessor 520, or outside SPU 500.

Decompression is important in the release of data such as video
and **audio** that is usually compressed before distribution and
whose decompression speed is important. In some cases,
information that is useful for usage monitoning purposes (such as...unit 530 may be
modelled after a USART or PCI
bus interface in the preferred embodiment. In this example, BIU
530 connects SPU 500 to **electronic** appliance system bus 653
shown in Figure 8. BIU 530 is designed to prevent unauthorized
access to internal components within SPU 500 and their
contents...general
kinds of memory.

(1) internal ROM 532;
(2) internal RAM 534; and
(3) external memory (typically RAM and/or disk supplied
by a host **electronic** appliance).

The 'internal ROM 532 and RAM 534 within SPU 500
provide a secure operating environment and execution space.

Because of cost limitations, chip fabrication...532 may comprise a
combination of a masked ROM 532a and an EEPROM and/or
equivalent 'flash" memory 532b. EEPROM or flash memory
532b is **used** to store items that need to be updated and/or
initialized, such as for example, certain encryption keys. An
additional benefit of providing EEPROIN1 and...of sufficient speed and
cost-effectiveness.

SPU External Memory
The SPU 500 can store certain information on memory
devices external to the SPU. If available, **electronic** appliance
600 memory can also be used to support any device external
portions of SPU 500 software. Certain advantages may be
gained by allowing the... ...external memory. As one

example, memory internal to SPU 500 may be reduced in size by using non-volatile read/write memory in the host **electronic** appliance 600 such as a non-volatile portion of RAM 656 and/or ROM 658.

Such external memory may be used to store SPU programs... ...stores in memory external to it.

SPU 500 can use a wide vaniety of different types of external memorv. For example, external memory may comprise **electronic** appliance secondary storage 652 such as a disk; external EEPROM or flash memory 658; and/or external RAM 656. External RAM 6056 may comprise an...disk) may not be necessary.

External memory used by SPU 500 may include two categories.

external memory dedicated to SPU 500, and memory shared with **electronic** appliance 600.

For some VDE implementations, sharing memory (e.g., **electronic** appliance RAM 656, ROM 658 and/or secondary storage 652) with CPU 654 or other elements of an **electronic** appliance 600 may be the most cost effective way to store VDE secure database management files 610 and information that needs to be stored external...may allow transitions from "SPU" mode to "normal" mode and back to "SPU" mode without exposing the content of secure memory 532, 534 or the **content** of re isters or other
91
memorv associated with microprocessor 2652 that mav contain information derived from secure mode operation.

In some example implementations, there...initialization sequence and preventing SPU dependence on any information held outside CPU/SPU 2650. This approach permits secret initialization information (e.a., keys for validating **digital** signatures on additional information to be loaded into secure memory 532, 534) to be held internally to CPU/SPU 2650 so that it is never...of the hardware tamper-resistant barrier 502.

240
appliance 600 has been described above. The following section describes an example of the software architecture of **electronic** appliance 600 provided by the preferred embodiment, including the structure and operation of preferred embodiment **'Rights**

Operating System' CROS") 602.

Rights Operating System 602
Rights Operating System ("ROS') 602 in the preferred
embodiment is a compact, secure, event-driven, services-based,
"component" oriented, distributed multiprocessing operating
system environment that integrates...and reciprocal
control information and mechanisms
supports conditional execution of controlled processes
within am, VDE node in a distributed. asynchronous
arrangement
control-led delegation of **rights** mi a distributed
environment
supports chains of handling and control
management environment for distributed, occasionally
connected but otherwise asynchronous networked
database
real time and time... ...mechanism for
organizing computer system resources that allows programmers
to create applications for computer systems more easilv. An
operating system does this by providing commonly **used**
functions, and by helping to ensure compatibility between
different computer hardware and architectures (,which may, for
example, be manufactured by different vendors). Operating
systems also... ...base hardware and peripheral devices.

ROS 602 is an Operating System Providing Significant
Advantages
ROS 602 is an 'operating system.' It manages the
resources of **electronic** appliance 600, and provides a commonly
used set of functions for programmers writing applications 608
for the **electronic** appliance. ROS 602 in the preferred
embodiment manages the hardware (e.g., CPU(s), memory(ies),
secure RTC(s), and encrypt/decrypt engines) within SPU 500.

ROS may also manage the hardware (e.g., CPU(s) and
- 248
memorY(ies j) within one or more general purpose processors
within **electronic** appliance 600. ROS 602 also manages other
electronic appliance hardware resources, such as peripheral
devices attached to an **electronic** appliance. For example,
referring to Figure 7. ROS 602 may manage keyboard 612,
display 614, modem 618, disk drive 620, printer 622, scanner
624. ROS... ...602 in the
preferred embodiment supports any number of local and/or
remote processors. Supported processors may include at least

two types: one or more **electronic** appliance processors 654,
and/or one or more SPUs 500. A host processor CPU 654 may
provide storage, database, and co=unications services. SPU
500... ...Additional host
and/or SPU processors may increase efficiencies and/or
capabilities. ROS 602 may access, coordinate and/or manage
further processors remote to an **electronic** appliance 600 (e.g., via
- 249
network or other communications link) to provide additional
processor resources and/or capabilities.

ROS 602 is services based. The...auditing of distributed information) is a controlled event
that
itself uses such control structures. This 'reflective" distributed
processing mechanism permits ROS 602 to securely distribute
rights and permissions in a controlled manner, and effectively
restrict the characteristics of use of information content. The
controlled delegation of **rights** in a distributed environment and
the secure processing techniques used by ROS 602 to support
this approach provide significant advantages.

Certain control mechanisms within ROS...be proVided i-n a
template format such as method options to an end-user. An
end-user may then customize the actual control information **used**
within guidelines provided by a distributor or content creator.

Modification and update of existing control structures is
preferably also a controllable event subject to auditing... ...at least three general
approaches to
integrating VDE functions into a new operating system,
potential.ly based on an eidsting operating system, to create a
Rights Operating System 602 including.

257
(1) Redesign the operating system based on VDE
transaction management requirements;
(2) Compile VIDE API functions into an e@dsting...in what order
and under which circumstances or conditions they should be
performed.

Instead of (or 'in addition to) integrating VDE functions
into/with an **electronic** appliance operating system, it would be
ible to pro 'de certain VDE functionality available as an
possi VI I
application running on a conventional operating system.

ROS Software Axchitecture
Figure 10 is a block diagram of one example of a software structure/architecture for **Rights** Operating System CROS') 602 provided by the preferred embodiment. In this example, ROS 602 includes an operating system ("OS') 'core' 679, a user Application Program... ...503 are self-contained computing and processing environments that may include their own operating systern kernel 688 including code and data processing resources. A given **electronic** appliance 600 may include any number of SPE(s) 503 and/or any number of HPE(s) 655. HPE(s) 655 and SPE(s) 503...secure.

In the preferred embodiment, HIPE 655 is a secure processing environment supported by a processor other than an SPU, such as for example an **electronic** appliance CPU 654 general-purpose microprocessor or other processing system or device. In the prefer-red embodiment. HPE 655 may be 'dered to "emulate" an... ...be provided in two types: secure and not secure. For example, it may be desirable to provide non-secure versions of HPE 655 to allow **electronic** appliance 600 to efficiently run non-sensitive VDE tasks using the fuH resources - 262 of a fast general purpose processor or Computer. Such non secure... ...a software-based tamper resistant barnier 674 may be created by software executing on general-purpose CPU 654. Such a "secure' HPE 655 can be **used** by ROS 602 to execute processes that. while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. The SPU 502 may be **used** to perform all truly secure processing, whereas one or more HPEs 655 may be **used** to provide additional secure (albeit possibly less secure than the SPE) processing using host processor or other general purpose resources that ma be available within an **electronic** appliance y
600. Any service may be provided by such a secure HPE 655. In 263
the preferred embodiment, certain aspects of 'channel processing' appears... ...storage device (e.g., a hard disk, memory card, etcJ to form internal test values to impede moving and/or copying HPE 655 to other **electronic** appliances 600; using kernel code that contains false branches and other complications 'in flow of control to disguise internal processes to some degree from disassemblv... ...sequences are not stored explicitly on storage devices and/or in active memory but rather are generated as needed; using code that "shuffles' memory locations **used** for data values based on operational parameters to complicate efforts to

manipulate such values; using any software and/or hardware memory management resources of **electronic** appliance 600 to "protect" the operation of HPE 655 from other processes,

- 264

functions, etc. Although such a software-based tamper resistant barrier 674 may... ...by one or more secure HPEs 655 executing on general-purpose CPUs 654. Some VDE processes may not be allowed to proceed on reduced-secuniry **electronic** appliances of this type if insufficient security is provided for the particular process involved.

Only those processes that execute completely within SPEs 503 (and in... ...truly secure. Memory and other resources exterriai to SPE 503 and HPEs 655 used to store and/or process code and/or data to be **used** in secure processes should only receive and handle that information in encrypted form unless SPE 503/HPE 655 can

- 265

protect secure process code ...679. They may also communicate messages directly with one another without messages going through OS 'core' 679,
Kernel 680 mav manaae the hardware of an **electronic** appliance 600. For example, it may provide appropriate drivers and hardware manacTers for interactingWith Linput/output and/or peripheral devices such as keyboard 612, display... ...732 may route these RPCs to kernel 680 or elsewhere (e.g., to HPE(s) 655 and/or

- 267

SPEW 5,03, or to remote **electronic** appliances 600, processors, or VDE participants) for processing. The API 682 may also service RPC requests by passing them to applications 608 that register to...628 for example), and routes one or more such data feeds appropriately while providing "translation' functions for real time data sent and/or received bv **electronic** appliance 600 to allow "transparency" for this ty 1
1 . pe of information analogous to the transparency prol@lded by redirector 684 (and/or it...modified control information set constitutes independent, secure delivery). For example, a content creator can produce a ROS 602 application that defines the circumstances required for **licensing** content contained within a VDE object 300. This application may reference structures provided by other parties. Such references

- 273

might, for example, take the form... ...deliverL'rg different data elements defining pricing to different users. This attribute of supporting multiple party securely. independently deliverable control information is

furidamental to enablinu **electronic** commerce, that is. defining of
a content and,,'or appliance control infor-manon set that
represents the requirements of a collection of independent
parties such... ...N-level subassembly 690(k +
N). The ability of ROS 602 to build component assemblies 690
out of other component assemblies provides great advantages in
terms of, for example, code/data reusability, and the ability to
allow different parties to manage different parts of an overall
component.

- 275
Each component assembly...distributor, then the person could establish a
price of zero instead ofthe price the content distributor 'intended
to charge. Similarly, if the element establishes an **electronic**
credit card, then an abilitv to substitute a different element
could have disastrous consequences 'in **terms** of allowing a person
to charge her usage to someone else's (or a non-existent) credit
card. These are merely a few simple examples...1100 that
perform the same or similar functions on different platforms,
thereby making the method scalable and/or portable across a
wide range of different **electronic** appliances.

UDEs 1200 and MDEs 1202 may store data for input to or
output from executable component assembly 690 (or data
describing such inputs and... ...1 100d) in this example 'include one
C)
'DTD" data elements 1108 (e.(7., 1108a, 1108b). "DTD"
or more t3
data elements 1108 may be **used**, for example, to inform load
module 1100a of the data elements included in MDE 1202 and/or
UDEs 1200a, 1200b. Furthermore, DTDs 1108 may be...in
a different PERC 8080)) to form a different component assembly
6900). Even though component assembly 6900) is formed from
some of the same components **used** to fon-n component assembly
690(k), these two component assemblies may perform completely
different processes in complete different ways.

As mentioned above, ROS 602... ...external media encrypted using local SPU 500
generated
and/or distributor provided keys.

ROS 602 also provides a tagging and sequencing scheme
that may be **used** within the loadable component assemblies 690
to detect tampering by substitution. Each element comprising a
- 284
component assembly 690 may be loaded into an SPU...implementation

investment and comple@dtv may be 1='Ited. The process of
17 surfacing" the full range of capabilities pro'@qided by ROS 602 in
terms of authoring, administrative, and artificial intelligence
applications may take place over time. Nloreover, already
designed functionality of ROS 602 may be changed or enhanced
at any time to adapt to changing needs or requirements.

- 286
More Detailed Discussion of **Rights** Operating System 602
Architecture
Figure 12 shows an example of a detailed architecture of
ROS 602 shown in Figure 10. ROS 602 may include a... ...take place
within an SPE 503 having an execution space within a physical
SPU 500 rather than a HPE 655 using software operating
elsewhere in **electronic** appliance 600.

As mentioned above, three basic components of ROS 602
are a kernel 680, a Remote Procedure Call (RPC) manager 732
- 287
and an... ...components, and the way they
interact with other portions of ROS 602, will be discussed below.

KerneI680
Kernel 680 manages the basic hardware resources of
electronic appliance 600, and controls the basic tasking provided
by ROS 602. Kernel 680 in the preferred embodiment may
include a memory manager 680a, a task deallocation, sharing and/or use of memory (e.g.,
RAM
656 shown in Figure 8) of **electronic** appliance 600, and may for
example provide virtual memory capabilities as required by an
electronic appliance and/or associated application(s). I/O
manager 680c may manage all input to and output from ROS
602, and may interact with drivers... ...to seamlessly
'de distributed and/or remote processing. In smaller scale
prov-1
instances of ROS 602, a simpler message passing IPC protocol
may be **used** to conserve resources. This may linuit the
configurability of ROS 602 services, but this possible limitation
may be acceptable in some **electronic** appliances.

The RPC structure allows services to be called/requested
without the calling process having to know or specify where the
service is physically provided... ...Procedure
Calis' (RPCs) from a service requestor, and routes the service
requests to a service provider(s) that can service the request. For
example, when **rights** operating system 602 receives a request

from a user application via user API 682, RPC manager 732 may
- 290
route the service ...admini trative objects;
IncominLr Administrative Objects Manager 756 services
requests relating to incoming administrative objects;
and
Communications Manager 776 services requests relating
to communications between **electronic** appliance 600
and the outside world.

Object Switch 734
Object switch 734 handles, controls and communicates
(both locally and remotely) VDE objects 300. In the...780 and a mail gateway
(manager) 782. Mail gateway 782 may include one or more mail
filters 784 to, for example, automatically route VDE related
electronic mail between object switch 734 and the outside world
electronic mail services. External Services Manager 772 may
interface to communications manager 776 through a Service
Transport Layer 786. Service Transport Layer 786a may enable
External...to accept requests.

1
RPC LOAD Call Example: SVC-LOAD (long service
1d)
This LOAD interface call is called by the RPC manager
732 during **rights** operating system 602 initialization. It permits
a service manager to load any dynamically loadable components
and to initialize any device and memory required by the...no longer valid) -or an error
number.

303
This UNLOAD interface call is called by a RPC manager
732 during shutdown or resource reallocation of **rights** operating
system 602. It permits a service to close any open connections,
flush buffers, and to release any operating system resources that
it may have...repository
728 or to redirector 692 (which in turn accesses the object in file
system 687).

- 318
Generallv. redirector 684 maps VDE object repository 728
content into preexisting calls to file system 687. The redirector
684 provides preexisting OS level information about a VDE
object 300, including mapping the object into...Service Manager 740 and associated user
notification exception interface ("pop up') 686 provides ROS 602
with an enhanced abilitv to communicate with a user of

electronic appliance 600. Not all applications 608 may be
- 319
designed to reSDond to messaging from ROS 602 passed through
API 682, and it may in... ...DLL), or it may be directly
linked with an applications's code- depending on an apphcation
programmer's implementation decision, and/or the type of
electronic appliance 600. The Notification Service Manager 740
may be implemented within API 682. These components
interface with Notification Service component 686 to provide a
transition...lookup between the names (and other information, such as for
example address, communications connection/routing
information, etc.) of other processing resources (e.g., other host
electronic appliances) and VDE node IDs. Services name service
provides a mapping and lookup between services names and
other pertinent information such as connection information (e... ...communications.

- 326
There are several important examples of the use of
Externall Services Manager 772. Some VDE objects may have
some or all of their **content** stored at an Object Repository 728 on
an **electronic** appliance 600 other than the one operated by a user
who has, or wishes to obtain, some usage **rights** to such VDE
objects. In this case, External Services Manager 772 may
manage a connection to the **electronic** appliance ...used to access VDE
objects, manv different techniques are possible. For example, the
VDE objects may be for-matted for use with the World Wide **Web**
protocols (HTN-IL. HTTP, and URL) by including relevant
headers, content tags, host ID to URL conversion (e.g., using
Name Services Manager 752) and... ...administrative object manager 754 receives
administrative ob'ects from object switch 734, object repository
manager 771 0 or other source for transmission to another VDE
electronic appliance. Outgoing administrative object manager
754 takes care of sending the outgoing object to its proper
destination. Outzoinc; administrative object manager 754 may
obta-L... ...transmitted
and other information related to transmission of objects.

Incoming Administrative Object Manager 756
Incoming administrative object manager 756 receives
administrative objects from other VDE **electronic** appliances 600
via communications manager 776. It may route the object to
object repository manager 770, object switch 734 or other
- 328
destination. Incoming administrative...to
create VDE objects 300 (administrative objects).

- 329

Figure 12A shows how object submittal manager 774 may
be used to communicate with a user of **electronic** appliance 600
to help to create a new VDE object 300. Figure 12A shows that
object creation may occur in two stages in the preferred...503 to create secure data control
structures). Container
manager 764 may then write the new object to object repository
687, and the user or the **electronic** appliance may "register" the
new object by including appropriate information within secure
database 610.

- 333
Communications Subsystem 776
Communications subsystem 776, as discussed above, may... ...time content
feed 684 from a cable. satellite or other telecommunications link.

Secure ProceBsing Environment 503
As discussed above in connection with Figure 12, each
electronic appilance ...ROS 602, and they
may themselves generate service requests to be satisfied by other
services within ROS 602 or by services provided by another VDE
electronic appliance 600 or computer.

In the preferred embodiment, an SPE 503 is supported by
the hardware resources of an SPU 500. An HPE 655 may... ...602 (although ROS 602
may be
restricted from -sendim: to an HPE certain highly secure tasks to
be executed on]%- within an SPU 500).

Some **electronic** ampliance 600 configurations might
include both an "PE 503 and an HPE 655. For example, the
HPE 655 could perform tasks that need lesser (or...unacceptable to
use a full "multi-threaded' data structure w-rite capabilities. For
example, a ty
, pe of "two-phase commit" processing of the type
used by database vendors may be **used** to allow data structure
sharing between processes. To implement this "two-phase
commit" process. each swap block may contain page addresses for
additional memorv blocks...

Claims:

1 A **rights** management appliance including:
a user input device,a user display device,at least one processor, andat least one element
defining a protected processingenvironment,characten'zed in that the protected processing

environmentstores and uses permissions, methods, keys, programs and/orother information to electronically manage **rights**.

2 In a **rights** management appliance including:

a user input device,a user display device,at least one processor, andat least one element defming a protected processingenvironment,a method of operating the appliance characterized by thestep of storing and using permissions, methods, keys, programsand/or other information to electronically manage **rights**.

3 A **rights** management appliance including at least one

processor element at least in part defining a protected processing- 995 environment, characterized in that the protected processingenvironment stores and uses permissions, methods, keys,programs and/or other information to electronically manage**rights**.

4 In a **rights** management appliance including at least one

processor element at least in part defining a protected processingenvironment, a method comprising storing and usingpermissions, methods, keys, programs and/or other informationto electronically manage **rights**.

5 An **electronic** appliance arrangement containing atleast

one secure processing unit and at least one secure databaseoperatively connected to at least one of said secure processingunit... ...atleast one aspect of appliance usage and control said usage basedat least in part upon protected appliance usage controlinformation.

6 In an **electronic** appliance arrangement containing at least

one secure processing unit and at least one secure databaseoperatively connected to at least one of said secure processing... ...one aspect of appliance usage and controlling szdd- 996 pCTfUS97/15243 usage based at least in part upon protected appliance usage control information.

7 An **electronic** appliance arrangement containing a

protected processing environment and at least one securedatabase operatively connected to said protected processingenvironment, said arrangement including means to... ...at least mi part upon protectedappliance usage control information processed at least in partthrough use of said protected processing environment.

8 In an **electronic** appliance arrangement containing a

protected processing environment and at least one securedatabase operatively connected to said protected processingenvironment, a method characterized by the... ...based at least in part upon protected appliance usagecontrol information processed at least in part through use of saidprotected processing environment.

9 An **electronic** appliance arrangement containing one or

more CPUs wherein at least one of the CPUs incorporates anintegrated secure processing unit, said arrangement storing997 protected appliance usage control information designed to besecurely processed by said integrated secure processing unit.

10 In an **electronic** appliance arrangement containing one ...of

storing and securely processing protected modular componentappliance usage control information with said integrated secureprocessing unit.

11 A method of compromising a distributed **electronic rights**

management system comprising plural nodes having protectedprocessing environments, characterized by the following steps:(a) exposing a certification private key,(b) passing at least one... ...key exposed by the exposing step,(c) creating a processing environment

based at least inpart on steps (a) and (b), andparticipating in distributed **rights** management using theprocessing environment created by step (c). - 998 . A processing environment for compromising a distributed**electronic rights** management system comprising plural nodeshaving protected processing environments, characterized by thefollowing:protocol passing means including an exposed certificationprivate key for passing at... ...defeating an initialization challenge/response security,and/or (b) exposing external communication keys, andmeans coupled to the security detecting means forparticipating in distributed **rights** management.

13 A method of compromising a distributed **electronic rights** management system comprising plural nodes having associatedprotected processing environments, characterized by the steps of.compromising the permissions record of an **electronic**container, andusing the compromised permissions record to access and/oruse **electronic** information.

14 A system for compromising a distributed **electronic rights** management system comprising plural nodes having associatedprotected processing environments, characterized by means for- 999 using a compromised permissions record of an **electronic**container for accessing and/or using **electronic** information.A method of tampering with a protected processingenvironment characterized by the steps ofdiscovering at least one system-wide key, andusing the...

18/K/17 (Item 5 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT
(c) 2009 WIPO/Thomson. All rights reserved.

Patent Applicant/Patent Assignee:

- **ELECTRONIC PUBLISHING RESOURCES INC...**

Country	Number	Kind	Date

Detailed Description:

...field 597(1), a user ID field 597(2), an
object ID field 597(3), a field containing a reference or other
identification to a "**right**' (i.e., a collection of events supported by
methods referenced in a PERC 808 and/or "user **rights** table" 464)
597(4), an event queue 597(5), and one or more fields 598 that
cross-reference particular event codes with channel detail records... ...the preferred
embodiment. In the preferred embodiment, a channel 594
- 343

provides event processing a particular object 300, a
Particular authorized user, and a particular "**right**" (i.e., type of
event). These three parameters may be passed to SPE 503. Part
of SPE kernel/dispatcher 552 executing within a "channel O... ...1127).

In the preferred embodiment, this 'blueprint" may comprise a
PERC 808 and/or URT 464. In may be obtained by using the
"Object, User, **Right**" parameters passed to the "open channel"
routine to "chain" together object registration table 460 records,
user/object table 462 records, URT 464 records, and PERC...write appropriate
information to channel header 596 (block
1129). Such information may include, for example, User ID,
- 344
Object]OD, and a reference to the "**right**' that the channel will
process. The preferred embodiment process may next use the
'blueprint" to access (e.g, the secure database manager 566
and/or... ...needed to respond to the
event. The number of channel detail records will depend on the
number of events that can be serviced by the "**right**," as specified
by the "blueprint" (i.e., URT 464). During this process, the
control method will construct "swap blocks" to, in effect, set up all...the
NVRAM 534b of SPU 500). These tags may be generated by key
and tag manager 558. They are used to, for example, check
access **rights** to, validate and correlate data elements. For
example, they may ...event summaries may be maintained,
analyzed and used by SPE 503 (HPE 655) or a VDE
adynini trator to determine and potentially Emit abuse of
electronic appliance 600. In the preferred embodiment, such
parameters may be stored in secure memory (e.g., within the
NVRAM 534b of SPU 500).

There are... ...and/or distributors for
overall budget. A VDE admini trator may register for event
- 370
summaries and an overall budget summary at the time an
electronic appliance 600 is initialized. The overall budget
summary may be reported to and used by a VDE admini trator
in determining distribution of consumed budget...

Claims:

1 A method for secure content delivery including:
a) encapsulating **digital** information within one or more**digital** containers;b) encrypting
at least one portion of said **digital**information; O associating at least partially secure
controlinformation for managing interaction with saidencrypted **digital** information

and/or the **digital**container;d) delivering one or more of said one or more **digital**containers to a **digital** information user;e) employing a protected processing environment forsecurely controlling decryption of at least a portion ofsaid **digital** information.

2 A system for secure content delivery including:

encrypting means for encrypting at least one portion of**digital** information;container processing means for encapsulating **digital**information within one or more **digital** containers and forassociating at least partially secure control information formanaging interaction with said encrypted **digital** information;921delivery means for delivering one or more of said one ormore **digital** containers to a **digital** information user; andat least one protected processing environment for securelycontrolling decryption of at least a portion of said **digital**information.

3 A method for secure **digital** information delivery

characterized by the steps of.- (a) encrypting at least a portion ofsaid **digital** information through the use of a first at least oneVDE node, (b) creating and encrypting, through the use of saidfirst at least one VDE node, control information to control use ofat least a portion of said **digital** information by plural, users, (c)securely providing said control information to said plural users,and (d) employing at least one VDE node different from said firstat least one VDE node to process at least portions of said controlinformation and to control use of said encrypted **digital**information by said users.

4 A system for secure **digital** information delivery

characterized by:a first at least one VDE node for encrypting at least aportion of said **digital** information,means for creating and encrypting, through the use of saidfirst at least one VDE node, control information to control use ofat least a portion of said **digital** information by plural, users,922mean for securely providing said control information tosaid plural users, andat least one VDE node different from said first at least oneVDE node for processing at least portions of said controlinformation and to control use of said encrypted **digital**information by said users.

5 A method for secure content delivery wherein at least

partially encrypted content is encapsulated within at least one**digital** container and the **digital** container is delivered to a **digital**information user, the method characterized by the steps ofassociating, with the encapsulated content and/or the**digital** container, at least partially secure control information formanaging interaction with the container and/or the content; andemploying a protected processing environment forsecurely encrypted content is encapsulated within at least one**digital** container and the **digital** container is delivered to a **digital**information user, the system characterized by:a data structure that associates, with the encapsulatedcontent and/or the **digital** container, at least partially secure923control information for managing interaction with theinformation; anda protected processing environment for securelycontrolling decryption of at least a portion of the encryptedcontent based at least in part on the control information.

7 A method for secure **digital** information delivery

characterized by the steps of. (a) encrypting at least a portion ofsaid **digital** information, (b) associating protected controlinformation to at least a portion of said **digital** information, and c)providing at least a portion of said encrypted **digital** informationto a first user and at least in part controlling use of at least aportion of said encrypted **digital** information through the use ofat least a portion of said protected control information,

whereinsaid first user further provides at least one of (a) a copy of said atleast a portion of said encrypted **digital** information, or (b) saidencrypted **digital** information, to a second user, and wherein saidsecond user associates further control information with saidencrypted **digital** information for use in controlling use of saidencrypted **digital** information by a third user.

8 A system for secure **digital** information delivery

characterized by:means for encrypting at least a portion of said **digital**information,924mesan for associating protected control information to atleast a portion of said **digital** information,means for providing at least a portion of said encrypted**digital** information to a first usermeans for at least in part controlling use of at least aportion of said encrypted **digital** information through the use ofat least a portion of said protected control information,mean for allowing the first user to provide at least one of(a) a copy of said at least a portion of said encrypted **digital**information, or (b) said encrypted **digital** information, to a seconduser, andmeans for allowing said second user to associate finthercontrol information with said encrypted **digital** information foruse in controlling use of said encrypted **digital** information by athird user.

9 A method for secure **digital** transaction management

including:a) encrypting **digital** information at a first location;b) enabling a first party to securely associate at leastone control with said information for use in ensuringat said consequencesof use of said information.

10 A system for secure **digital** transaction management

including interconnected structures for performing the followingfimctions:a) encrypting **digital** information;b) enabling a first party to securely associate at leastone control with said information for use in ensuringat least one consequence of... ...toa further party; ande) decrypting at least a portion of said information; andf) securely ensuring said consequences.926. A system for secure **digital** tran action managementwherein **digital** information is encrypted by a first party at a firstlocation and distributed, characterized by:a first protected processing environment for enabling thefirst party... ...at least one consequence of use of the information based at leastin part on the first and further controls.

12 A method for secure **digital** transaction management

wherein **digital** information is encrypted by a first party at a firstlocation and distributed, characterized by the following steps:enabling the first party to securely associate... ...portion of said information whilecontrolling at least one consequence at least in part on thetransmitted controls.927. A method for securely automating distributed**electronic** processes including:a) providing secure, interoperable, general purpose**rights** management processing means to multiple,parties;b) establishing secure process management controls forautomatically, at least partially remotely, andsecurely supporting requirements related to**electronic** events;O securely distributing process management controlsto party sites;d) securely maintaining at least a portion of saidprocess management controls under the control ofparty processing mean at said party sites;e) automatically managing **electronic** processes at saidparty sites to enforce interests related to said**electronic** content.

14 A system for securely automating distributed

electronic processes including:interoperable **rights** management processing meandisposed at multiple parties' sites;control establishing mean for establishing secure

processmanagement controls; for remotely, automatically, and securelysupporting requirements related to **electronic** events; and for928securely distributing process management controls to partysites;security mean for securely maintRinin at least a portionof said process management controls under the control ofprocessing means at said party sites; andmanaging means for automatically managing **electronic**processes at plural party sites to enforce interests related to said**electronic** events.

15 A method for automating distributed **electronic** processes using interoperable processors at multiple sites,characterized by the following steps:securely distributing, to the processors, processmanagement controls for automatically, and securely supportingrequirements related to **electronic** events;securely maintaining at least a portion of said processmanagement controls under the control of the processors; andautomatically managing, in a distributed manner withthe processors, **electronic** processes at the multiple sites toenforce interests related to **electronic** events.

16 A system for automating distributed **electronic** processes using interoperable processors at multiple sites,characterized by the following:929distributing means connected to the processors forsecurely distributing, to the processors, process managementcontrols for remotely, automatically, and securely supportingrequirements related to **electronic** events;process control means for securely maintaining at least aportion of said process management controls under the control ofthe processors; andmanagement means for automatically managing, in adistributed manner with the processors, **electronic** processes atthe multiple sites to enforce the interests related to the **electronic**events.

17 A method of securely enforcing a **rights** seniority system characterized by the steps ofallowing a first user to create at least one control over**electronic** content; andallowing a second user to contribute at least one furthercontrol over **electronic** content and/or alter the control in place,the second control being subject to the first control.

18 A system for securely enforcing a **rights** seniority system characterized by:a first secure environment for allowing a first user tocontribute at least one control over **electronic** content; and930a second secure environment for allowing a second user tocontribute at least one further control over **electronic** contentand/or alter the control in place, the second control being subjectto the first control.

19 A method of securely enforcing a **rights** seniority system characterized by the step of allowing a first user to createat least one **electronic** control that at least in part dictates the**rights** a second user has to create further **electronic** controls overthe use of and/or access to **electronic** content.

20 A system for securely enforcing a **rights** seniority system characterized by at least one mean for allowing a firstuser to create at least one **electronic** control that at least in partdictates the **rights** a second user has to create further **electronic**controls over the use of and/or access to **electronic** content.2 1. A method for employing protected processingenvironments including:a) distributing interoperable protected processingenvironments to plural parties;b) providing a first interoperable protected processingenvironment for use by a first party to enable saidparty to (a) encrypt **digital** information, and (b)931create control information for managing at least oneaspect of use of said **digital** information;c) encrypting said **digital** information in

response toone or more instructions from said first party;d) making said **digital** information available to a secondparty;e) through the use of a second interoperable protectedprocessing environment, satisfying requirementsenforced by said control information and allowingsaid second party to use at least a portion of said**digital** information;f) through the use of said second interoperableprotected processing environment securely reportinginformation reflecting at least one aspect of saidsecond party use of said **digital** information.

22 A system for employing protected processing environments including:interoperable protected processing environmentsdistributed to plural parties, including a first interoperableprotected processing environment for use by a first party toenable said party to (a) encrypt **digital** information, and (b) createcontrol information for managing at least one aspect of use ofsaid **digital** information, and further including a secondinteroperable protected processing environment;932means for encrypting said **digital** information in responseto one or more instructions from said first party, and for makingsaid **digital** information available to a second party;means for a second interoperable protected processingenvironment to satisfy requirements enforced by said controlinformation and to allow said second party to use at least aportion of said **digital** information; and to securely reportinformation reflecting at least one aspect of said second partyuse of said **digital** information.

23 A method for employing protected processing environments distributed to plural parties characterized by thefollowing steps:using a first protected processing environment to encrypt**digital** information, and control information specifyingrequirements for managing at least one aspect of use of said**digital** information;using a second protected processing environmentinteroperable with the first protected processing environment toenforce the requirement specified by said control information andconditionally allowing use of at least a portion of said **digital**information; andusing the second protected processing environment toreport information reflecting at least one aspect of use of said**digital** information.933. A system for employing protected processingenvironments distributed to plural parties characterized by:a first protected processing environment to encrypt **digital**information, and for handling control information specifyingrequirements for managing at least one aspect of use of said**digital** information;a second protected processing environment interoperablewith the first protected processing environment for enforcing atleast one requirement specified by said control information andconditionally allowing use of at least a portion of said **digital**information; and for reporting information reflecting at least oneaspect of use of said **digital** information.

25 A secure network architecture comprising multiple cooperating interconnected nodes having protected processingenvironments, at least a portion of said nodes being able to...software defming protected processing environments, andproviding, with a secure database server, information forprocessing by the network workstation protected processingenvironments.

29 A distributed **electronic rights** management system comprising plural nodes having protected processingenvironments, characterized in that at least one of the pluralnodes provides a protected processing environment that...
...server function for a client comprising at least a portion of theprotected processing environment of at least one other node.

30 In a distributed **electronic rights** management system
comprising plural nodes having protected processingenvironments, a method
characterized by providing, with at leastone of the plural nodes, a protected processing...
...for a client comprising at least a portion of the protectedprocessing environment of at
least one other node.
31 A method for securely managing **electronic**
negotiations related to **electronic** commerce value chain activitiesincluding:a) employing
a protected processing environment by afirst party to securely specify rules and/or
controlsfor managing an **electronic** commerce process;b) securely making said specified
n3les and/or controlsavailable to a second party;c) employing a protected processing
environmentdifferent from said... ...said second party;936d) employing said protected
processing environment tosecurely electronically negotiate at least oneaggregate rules
and/or controls set representing the**electronic** interests of both said first party and
saidsecond party;e) employing a protected processing environment tomanage said
electronic commerce process consistentwith at least a portion of said aggregate rules
and/orcontrols set.
32 A system for securely managing **electronic** negotiations
related to **electronic** commerce value chain activities including:a first party's protected
processing environment forsecurely specifying rules and/or controls for managing
an**electronic** commerce process, and for securely making saidspecified rules and/or
controls available to a second party;a second partys protected processing
environmentdifferent from... ...s and the second party'sprotected processing environment
for securely electronicallynegotiating at least one aggregate rules and/or controls
set937representing the **electronic** interests of both ...andsaid second party; andat least one
of the first party's and thesecond party'sprotected processing environment including
means for managingsaid **electronic** commerce process consistent with said at least
aportion of said aggregate rules and/or controls set.
33 A method for securely managing **electronic**
negotiations related to **electronic** commerce value chain activitiesthrough use of first and
second protected processing environmentcharacterized by:using the first environment,
securely specifying rulesand/or controls for managing an **electronic** commerce
process;using the second environment, further securely specifyingrules and/or controls
for managing at least one commerce processrelated to the commercial interests... ...least
one of the first and second protectedprocessing environments to securely electronically
negotiate atleast one aggregate rules and/or controls set representing the**electronic**
interests of the first party and said second party; andemploying at least one of the first
and second protectedprocessing environment to manage said **electronic**
commerceprocess consistent with at least a portion of said aggregate rulesand controls
set.938. A system for securely managing **electronic** negotiationsrelated to **electronic**
commerce value chain activities through useof first and second protected processing
environmentcharacterized by:the first environment including means for
securelyspeciPjing rules for managing an **electronic** commerce process;the second
environment including mean for furthersecurely specify rules for managing at least one
commerceprocess related to the commercial interests of... ...of the first and second
protected processingenvironments including means for securely electronicallynegotiating
at least one aggregate rules set at least partiallyrepresenting the **electronic** interests of

said first party and saidsecond party; andat least one of the first and second protected processingenvironment including means for managing said **electronic**commerce process consistent with said at least a portion of saidaggregate rules set.

35 A method for managing a distributed **electronic**
commerce environment including:a) establishing a secure, certificate authority forauthenticating a user identity for an **electronic**939commerce participant wherein said identity includesone or more user class parameters;b) certifying said user identity through the use of oneor more certificates enabled by said certificateauthority;c) controlling the use of distributed **electronic**information based at least in part on class parameterinformation included in such certified identity.

36 A system for securely managing a distributed
electronic commerce environment including:means for establishing a user identify for an **electronic**commerce participant wherein said identity includes one or moreuser class parameters;a certificate authority for authenticating such useridentity by certifying said user identity through the use of one ormore certificates enabled by said certificate authority; andmeans for controlling the use of distributed **electronic**information based at least in part on class parameter informationincluded in such certified identity.

37 A method for securely managing a distributed
electronic commerce environment to allow interaction with an**electronic** commerce participant having a user identity that iscertified by a certificate authority, characterized by:940establishing a user identity;certifying the user identity and... ...the user identity, at least one user classparameter, wherein said certified class parameter, at least inpart, is used to control use of distributed **electronic** information.

38 A system for managing a distributed **electronic**
commerce environment to allow interaction with an **electronic**commerce participant having a certified user identity,characterized by:mean for associating at least one user class parameterwith an established user identity;means for ascertaining the authenticity of the user identityand/or the user class parameter; andmean for controlling use of distributed **electronic**information based at least in part on said status.

39 A system as in claim 38 wherein the class parameter
represents the user@s age, and the controlling means includesmeans for controlling the use of distributed **electronic**information based on the user's age.

40 A method of securely establishing user identity
through use of certificates, the method characterized by:941presenting an **electronic** token reflecting at least one userclass characteristic;determining whether an **electronic** certificate authenticatesthe user class characteristic reflected by the token; andusing the token as a basis for granting **rights**.

41 A system for identifying a user through use of
certificates, the system characterized by:means presenting an **electronic** token reflecting at leastone user class characteristic;means for obtaining an **electronic** certificate;means for determining whether the **electronic** certificateauthenticates the user class characteristic reflected by the token;andmeans for using the certified, authenticated token as abasis for granting **rights**.

42 A system for securely managing a distributed
electronic commerce environment including:means for identifying an **electronic** commerce participantby specifying at least one user category;means for authenticating

such user identity; andmeans for controlling the use of distributed **electronic**information based at least in part on the user category.942. A method for securely managing a distributed**electronic** commerce environment to allow interaction with an**electronic** commerce participant, characterized by:establishing a user identity and an associated user classparameter; andusing the class parameter to, at least in part, control use ofdistributed **electronic** information.

44 A system for managing a distributed **electronic**
commerce environment to allow interaction with an **electronic**commerce participant, characterized by:means for associating at least one user class parameterwith a user identity;means for authenticating the user identity and/or the userclass parameter; andmeans for controlling use of distributed **electronic**information based at least in part on said status.

45 A system as in claim 44 wherein the class parameter
represents the user's age, and the controlling mean includesmean for controlling the use of distributed **electronic**information based on the user's age.

46 A method of securely establishing user identity, the
method characterized by:943presenting an **electronic** token reflecting at least ...class characteristic;determining the user class characteristic reflected by thetoken is authentic; andusing the token as at least a partial basis for granting**rights**.

47 A system for securely establishing user identity
characterized by:mean presenting an **electronic** token reflecting at leastone user class characteristic;authenticating the user class characteristic reflected by thetoken; andmean for using the authenticated token as a basis forgranting **rights**.

48 A method of authenticating a user identity, the method
characterized by:receiving a certificate request and associated user identity;andissuing an **electronic** certificate for use in authenticating atleast one user class characteristic associated with the useridentity for granting **rights** based on the user class characteristic.944. A system for authenticating user identity,characterized by:mean for receiving a certificate request and associateduser identity; andmeans for issuing an **electronic** certificate for use inauthenticating at least one user class characteristic associatedwith the user identity for granting **rights** based on the user classcharacteristic.

50 A method of securely establishing user identity, the
method characterized by:receiving a certificate request; andissuing an **electronic** certificate specifying at least one userclass characteristic.

51 A system for securely establishing user identity
through use of certificates, characterized by:means for receiving a certificate request and associateduser identity; andmeans for issuing an **electronic** certificate specifying atleast one user class characteristic.945. A method or system of managing **rights** characterizedin that a cryptographically signed token is used to certifymembership in a class, the token is authenticated, and the classmembership represented by the token is used as a basis forgranting and/or withholding **rights** and/or permissions.

53 A method or system of managing **rights** characterized
in that a cryptographically signed token is used to certifymembership in a class, the status of such token is ascertained,and the class membership represented by the token is used as abasis for allowing a user presenting the token to create **electronic**rules.

54 A method or system of managing **rights** characterized

in that a cryptographically signed token is used to certifymembership in a class, the token is validated, and the classmembership represented by the token is used as a basis forallowing a user presenting the token to exercise **rights** under**electronic** rules.

55 A method for enabling a distributed **electronic** commerce **electronic** agreement system including:a) enabling distributed, interoperable secure clientprotected processing environment nodes;946b) establishing at least one system wide securecommunications key;c) employing public key encryption for communicationsbetween plural client nodes;d) supporting the delivery of **electronic** controlinformation by individual clients wherein saidcontrol information at least in part specffies theirrespective **electronic** commerce agreement **rights**;e) supporting at least one protected processingenvironment for determining the respective and/orcollective **rights** of said clients by establishing one ormore **electronic** agreements based at least in part onsaid secure delivery of **electronic** control information;f) employing a secure software container data controlstructure for ensuring persistent maintenance of the**electronic rights** of the clients;g) using secure software containers which provide fordata structures that support rules and/or controlscorresponding to **electronic** commerce modelagreement enforcement.

56 A distributed **electronic** agreement system including:
plural distributed, interoperable secure client protectedprocessing environment nodes for supporting delivery of**electronic** control information by individual clients wherein said947control information at least in part specifies said client'srespective **electronic** commerce model agreement **rights**, and foremploying public key encryption and authentication forcommunications between said plural client nodes;means coupled to said nodes for establishing at least onesystem wide secure communications key; andat least one protected processing environment for:(a) determining the respective and/or collective **rights** of**electronic** commerce model clients by establishingone or more **electronic** agreements based at least inpart on said secure delivery of **electronic** controlinformation;(b) employing a secure software container data controlstructure for ensuring persistent maintenance of the**electronic rights** of commerce model clients; and(c) using secure software containers which provide fordata structures that support controls correspondingto **electronic** commerce model agreementenforcement.

57 A method for enabling a distributed **electronic** commerce **electronic** agreement system including distributed,interoperable secure client protected processing environmentnodes employing at least one system wide secure communicationskey, employing public key encryption and... ...for948communications between plural client nodes, and employing ancertification authority for establishing client identity, the methodcharacterized by:supporting the, secure delivery of **electronic** commercemodel agreement **rights** control information;determining the respective and/or collective **rights** of**electronic** commerce model clients by establishing one or more**electronic** agreements based at least in part on said securedelivery of the **electronic** control information;employing a secure software container data controlstructure for ensuring remote, persistent maintenance of the**electronic rights** of commerce model clients; andusing secure software containers which provide for datastructures supporting rules and controls corresponding to**electronic** commerce model agreement enforcement.

58 A distributed **electronic** commerce **electronic** agreement system including: Idistributed, interoperable secure client protectedprocessing

environment nodes employing at least one systemwide secure communications key, employing public keyencryption and authentication for communications betweenplural client nodes, employing an certification authority forestablishing client identity, and supporting the, secure delivery of**electronic** commerce model agreement **rights** control information;949means disposed in at least one node for determining therespective and/or collective **rights** of **electronic** commerce modelclients by establishing one or more **electronic** agreements basedat least in part on said secure delivery of the **electronic** controlinformation; andmeans disposed in at least one node for employing a securesoftware container data control structure for ensuring remote,persistent maintenance of the **electronic rights** of commercemodel clients, and for using secure software containers whichprovide for data structures supporting rules and controlscorresponding to **electronic** commerce model agreement enforcement.

59 A method of securely handling **electronic** currency characterized by the following steps:packaging **electronic** currency within a software container,anddelivering the software container as payment for goods orservices.

60 A system for securely handling **electronic** currency characterized by:means for packaging **electronic** currency within a softwarecontainer, and950means for delivering the software container as payment forgoods or services.

61 A method or system for managing **rights** within an organization characterized in that **electronic** containers aredistributed within the organization, the **electronic** containershaving controls associated therewith, the controls enforcing, atleast in part, an organizational hierarchy relating to the use ofthe containers and/or the contents thereof.

62 A method of organizational **rights** management characterized by the steps ofdistributing an **electronic** container within an organizationandrestricting usage, access and/or further distribution of the**electronic** container or the contents thereof within or outside ofthe organization based on **electronic** controls associated with the**electronic** container.

63 A system for organizational **rights** management characterized by:means for distributing an **electronic** container andmeans for restricting usage, access and/or furtherdistribution of the **electronic** container or the contents thereof951within or outside of the organization based on **electronic** controlsassociated with the **electronic** container.

64 A method of organizational **rights** management characterized by the steps of.distributing **electronic** containers within an organization,andusing the **electronic** containers, at least in part, toadmini ter content usage by persons within the organization.

65 A system for organizational **rights** management characterized by:means for distributing **electronic** containers within anorganization, andmeans for using the **electronic** containers, at least in part,to administer content usage by persons within the organization.

66 A method of organizational **rights** management characterized by the steps ofdistributing **electronic** containers within an organization,andusing the **electronic** containers, at least in part, toadminister use of money within the organization.

67 A system for organizational **rights** management

characterized by **electronic** containers distributed within an952organization for, at least in part, administering use of moneywithin the organization.

68 A method of organizational **rights** management characterized by the steps of:distributing protected processing environments within anorganization, andusing the environments to, at least in part, to administercontent usage by persons within the organization.

69 A system for organizational **rights** management characterized by protected processing environments distributedwithin an organization, for, at least in part, admini teringcontent usage within the organization.

70 A method of organizational **rights** management characterized by the steps of:distributing protected processing environments within anorganization, andusing the processing environments to, at least in part, toadmini ter use of money by persons within the organization.7 1. A system for organizational **rights** managementcharacterized by plural protected processing environments953distributed within an organization for, at least in part,achnini tering use of money within the organization.

72 A **rights** management appliance including:
a user input device,a user ...a protected processingenvironment,characterized in that the protected processing environmentstores and uses permissions, methods, keys, program and/orother information to electronically manage **rights**.

73 In a **rights** management appliance including:
a user input device,a user display device,at least one processor, andat least one element defining a protected processingenvironment,a method of operating the appliance characterized by thestep of storing and using permissions, methods, keys, programsand/or other information to electronically manage **rights**.

74 A **rights** management appliance including at least one processor element at least in part defining a protected processing954environment, characterized in that the protected processingenvironment stores and uses permissions, methods, keys,program and/or other information to electronically manage**rights**.

75 In a **rights** management appliance including at least one processor element at least in part defining a protectedprocessing environment, a method comprising storing and usingpermissions, methods, keys, program and/or other informationto electronically manage **rights**.

76 A method of electronically storing information in a repository and distributing it on request, characterized in thatthe information is protected by associating **electronic** controlswith the information, the **electronic** controls serving to enforce**rights** in the information.

77 A system for electronically storing information in a repository and distributing it on request, characterized by meanfor protecting information by associating **electronic** controls withthe information, and further including mean for using the**electronic** controls to enforce **rights** in the information.955. A self-protecting **electronic** container comprising:an **electronic** container structure for containing **digital**information, andan **electronic** protection mechanism that protects ordestroys the **digital** information in the event of tampering.

79 A method for a self-protecting **electronic** container comprising an **electronic** container structure for cont**digital** information, the method

characterized by detecting anattempt at tampering and protecting or destroying the **digital**information in the said attempt.

80 A method of creating a self-protecting container system comprising:providing at least one property,providing at least one... ...the property and/or attribute, andencapsulating the property, the attribute, thecryptographic key and the organizational structure, eitherexplicitly or by reference, into an **electronic** container structure.

81 A self-protecting container system comprising:
at least one property,956at least one attribute,at least one cryptographic key, andat least one orgam ational structure relating the key to theproperty and/or attribute.

82 A distributed **electronic rights** management system comprising plural nodes having protected processingenvironments, characterized in that each node can perform selfadmini tering processes in response to **electronic** components.

83 A self-administering **electronic** component comprising:
at least one method for performing at least a portion of atran action,at least one method for generating audit information, andat least one method for securely receiving and interpretingadmini trative information.

84 A self-admini tering **electronic** component performing the following methods:at least one method for performing at least a portion of atransaction,at least one method for generating audit information, andat least one method for securely receiving and interpretingadministrative information.957. A self-describing **electronic** component defining at leastone parameter and/or fimction, characterized in that thecomponent includes at least one secure, descriptive portion usedto create a human readable interface describing the parameterand/or function.

86 A method for processing a self-describing **electronic** component defining at least one parameter and/or function,characterized by the step of creating, at least in part with thecomponent, a human readable... ...parameterand/or fimction based at least in part on at least one secure,descriptive portion of the component.

87 A method of performing an **electronic** tran action comprising:receiving plural components,electronically detecting the occurrence of an event,determining, based on the event, a subset of the pluralreceived components to process the event, andperforming, in response to the event, at least one **electronic**process based on the component subset.

88 A system for performing an **electronic** transaction comprising:means for receiving plural components,958mean for electronically detecting the occurTence of anevent,means for determining, based on the event, a subset of theplural received components to process the event, andmeans for performing, in response to the event, at least one**electronic** process based on the component subset.

89 A distributed transaction processing method characterized by the following steps:receiving a first **electronic** component at a first location,receiving a second **electronic** component at a secondlocation,electronically detecting occurrence of an event at the firstlocation,processing, in response to the event detection, a firstportion of an **electronic** transaction at the first location based atleast in part on the first **electronic** component,securely transmitting at least one signal from the firstlocation to the second location, andprocessing at least a second portion of the **electronic**tr.qn action at the second location based at least in part on thesecond **electronic**

component.959. A method as in claim 89 further characterized by:sending at least one signal from the second location to thefirst location, andperforming at least a third portion of the **electronic**transaction at the first location based at least in part on receipt ofthe signal from the second location.

91 A distributed transaction processing system characterized by:means at a first location for receiving a first **electronic**component, for electronically detecting occurrence of an event, forprocessing, in response to the event detection, a first portion of an**electronic** transaction at the first location based at least in parton the first **electronic** component, and for securely transmittingat least one signal from the first location to a second location; andmeans at the second location for receiving a second**electronic** component, and for processing at least a second portionof the **electronic** transaction based at least in part on the second**electronic** component.

92 A system as in claim 91 further characterized by:
means at the second location for sending at least one signalfrom the second location to the first location, and960means at the first location for performing at least a thirdportion of the **electronic** transaction at the first location based atleast in part on receipt of the signal from the second location.

93 A distributed **electronic rights** management system comprising plural nodes having protected processingenvironments, characterized in that each node can perform**electronic** processes in response to receipt and assembly of**electronic** components, and the node authenticates each of the**electronic** components before assembling them.

94 A distributed **electronic rights** management method comprising:performing, with at least one protected processingenvironment, **electronic** processes in response to receipt andassembly of **electronic** components, andauthenticating, within the protected processingenvironment, each of the **electronic** components beforeassembling them.

95 A method as in claim 94 wherein the authenticating step includes the step of obtaining a corresponding certificatefrom a certifying authority.961. A distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, characterized in that each node can perform**electronic** processes in response to receipt and assembly of**electronic** components, and the node authenticates each of the**electronic** components by obtaining a corresponding certificatefrom a certifying authority.

97 In a distributed **electronic rights** management system comprising plural nodes having protected processingenvironments, a certifying authority that issues certificatesallowing each node to authenticate **electronic** components beforeassembling them to perform and/or control **electronic rights**management processes.

98 In a distributed **electronic rights** management system comprising plural nodes each having a protected processingenvironment, a method characterized by the step of issuingcertTicates allowing each node to authenticate **electronic**components before assembling them to perform and/or control**electronic rights** management processes.

99 A distributed **electronic rights** management system comprising plural nodes having protected processingenvironments, characterized in that

said nodes enforce usage962and/or access controls and is capable of electronically obt i 4compensation from a user and/or other processing of usageinformation for subsequent tran fer to **rights** holders.100. In a distributed **electronic rights** management systemcomprising plural nodes having a protected processingenvironment, a method characterized by the step of enforcingusage and/or access controls and electronically obtainingcompensation from a user and/or other processing of usageinformation for subsequent transfer to **rights** holders.101. A distributed **electronic rights** management systemcomprising plural nodes each having a protected processingenvironment, characterized in that each node enforces usageand/or access controls based on receipt of information frommultiple other nodes.102. A distributed **electronic rights** management methodcharacterized by the step of enforcing, with a protectedprocessing environment, usage and/or access controls based onreceipt of information from multiple other nodes.103. A distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, characterized in that said nodes are capable of at963least temporarily extending **electronic** credit to an associateduser for use in compensating **rights** holders.104. In a distributed **electronic** zights management systemcomprising plural nodes having protected processingenvironments, a method of operating the environmentcharacterized by the step of at least temporarily extending**electronic** credit to an associated user for use in compensating**rights** holders.105. A distributed **electronic rights** management systemcomprising plural nodes each having a protected processingenvironment, characterized in that said nodes are capable ofrequesting and obtaining a user-specific **electronic** creditassurance from a clearinghouse before granting the user **rights** toaccess and/or use electronically protected information.106. In a distributed **electronic rights** management systemcomprising plural nodes each having a protected processingenvironment, a method characterized by the step of requestingand obtaining a user-speciRc **electronic** credit assurance from aclearinghouse before granting the user **rights** to access and/or useelectronically protected information.964. A distributed **electronic rights** management systemcomprising plural nodes each having a protected processingenvironment, characterized in that each node is capable ofperforming and/or requesting an **electronic** debit or credittransaction as a condition to granting the user **rights** to accessand/or use electronically protected information.108. In a distributed **electronic rights** management systemcomprising plural nodes each having a protected processingenvironment, a method characterized by the step of performingand/or requesting an **electronic** debit or credit transaction as acondition to granting the user **rights** to access and/or useelectronically protected information.109. A distributed **electronic rights** management systemcomprising plural nodes each having a protected processingenvironment, characterized in that each node can maintain anaudit trail of user activities for reporting to a centralized location,the centralized location analyzing the user activities based on theaudit trail.110. In a distributed **electronic rights** management systemcomprising plural nodes each having a protected processingenvironment, a method characterized by the steps of.965maintainin , a plural locations, audit trails... ...useractivities for reporting to a centralized location, andanalyzing, at the centralized location, the user activitiesbased on the audit trail.111. A distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, characterized in that said node can monitor useractivities and trigger the occurrence of unrelated events based onthe user

activities and/or the **electronic** controls that associatethe user activities with the unrelated events.112. A system as in claim 111 wherein the unrelated eventis activation of an... ...a secure container.114. A system as in claim 111 wherein the unrelated eventis use of the protected processing environment.115. In a distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, a method characterized by the step of monitoring user activities at said nodes, and triggering the occurrence of966unrelated events based on the user activities and **electronic**controls that associate the user activities with the unrelatedevents.116. A method as in claim 115 wherein the unrelatedevent is at least one ofactivation of an application program,use of a secure container, anduse of the protected processing environment.117. A method of compromising a distributed **electronicrights** management system comprising plural nodes havingprotected processing environments, characterized by thefollowing steps:exposing a certification private key to allow a person topass... ...and/or (b) exposing externalcommunication keys,creating a processing environment based at least in part onthe above-mentioned steps, andparticipating in distributed **rights** management using theprocessing environment.967. A processing environment for compromising adistributed **electronic rights** management system comprisingplural nodes having protected processing environments,characterized by the following:means including an exposed certification private key topass a challenge/response... ...for defeating at least one of (a) an initializationchallenge/response security, and/or (b) exposing externalcommunication keys, andmeans for participating in distributed **rights** management.119. A method of compromising a distributed **electronicrights** management system comprising plural nodes havingprotected processing environments, characterized by the step ofcompromising the permissions record of an **electronic** containerand using the compromised permissions record to access and/oruse **electronic** information.120. A system for compromising a distributed **electronicrights** management system comprising plural nodes havingprotected processing environments, characterized by mean forusing a compromised permissions record of an **electronic**container for accessing and/or using **electronic** information.968. A method of tampering with a protected processingenvironment characterized by the steps of:discovering at least one system-wide key, andusing... ...one compromised system-wide key to decrypt and compromisecontent and/or admini trative information of a protectedprocessing environment without authorization.123. A distributed **electronic rights** management systemcomprising plural nodes having protected process'environments, characterized in that said nodes can electronicallyfingerprint content before releasing it in unprotected form.124. In a distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, a method characterized by performing, in at leastone of the nodes, the step of electronically fingerprinting contentbefore releasing it in unprotected form.125. A distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, characterized in that said nodes can embed,969within the **electronic** content, an **electronic** fingerprint contspecified information identif@ing a content **rights** holder and/oran indication of origin before including the content in an**electronic** container or allowing access to such content.126. In a distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, a method characterized by the step of embedding,within **electronic** content, an **electronic** fingerprint contspecified

information, including information identifying a content**rights** holder and/or an indication of origin before including the**content** in an **electronic** container or allowing access to such**content.**127. A distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** characterized in that the system includes one or**more** usage clearinghouses that receive usage information from**one** or more of the plural nodes.128. In a distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** a method characterized by the step of receiving,**with** a usage clearinghouse, usage information from one or more**of** said plural nodes.970. A distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** characterized in that the system includes one or**more** financial clearinghouses that receive financial information**relating** to the use of or access to content from one or more of**nodes.**130. In a distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** a method characterized by the step of receiving,**with** one or more financial clearinghouses, financial information**from** one or more of the plural nodes.131. A distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** characterized in that the system includes one or**more** analysis clearinghouses that receive information from one**or** more of the plural nodes and analyzes the received**information.**132. In a distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** a method characterized by the step of receiving,**with** one or more analysis clearinghouses, information from... ...**or** more of the plural nodes and analyzing the received**information,**133. A method of processing information pertaining to the**use** of or access to **electronic** content wherein such information is**received** from one or more nodes having protected processing**environments.**134. A method of providing credit for interaction with**content** to a protected processing environment node.135. A distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** characterized in that the system includes one or**more** clearinghouses that tran mits **rights** and/or permissio**information** to one or more of the plural nodes.136. In a distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** a method characterized by the step of transmitting**rights** and/or permissioning information from a clearinghouse to**one** or more of the plural nodes 972. A distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** characterized in that the system includes one or**more** clearinghouses that periodically transmit cryptographic**material** to one or more of said nodes, the cryptographic material**renewing** and/or replacing expiring cryptographic material.138. In a distributed **electronic rights** management system**comprising** plural nodes having protected processing**environments,** a method characterized by the step of periodically**tran** mitting cryptographic material from one or more**clearinghouses** to one more of said nodes, the cryptographic**material** renewing and/or replacing expiring cryptographic**material.**139. A secure **electronic** container characterized in that**the** container contains **electronic** controls for controlling the use**of** and/or access to **electronic** content that is external to the**container.**140. A method comprising:accessing **electronic** controls within a secure **electronic**container; and973using the controls for at least in part controlling the use of**and/or** access to **electronic** content that is external to the**container.**141. A secure

electronic container. characterized in thatthe container contains **electronic** controls for controlling, at leastin part, the use of and/or access to distributed **electronic** content.142. A method comprising:accessing **electronic** controls within a secure **electronic**container; andusing the controls for controlling, at least in part, the use ofand/or access to distributed **electronic** content.143. A secure **electronic** container characterized in thatthe container contains **electronic** controls that cause **electronic**content to expire on a time-dependent basis.144. A method for processing a secure **electronic** containerincluding the step of causing, at least in part based on **electronic**controls within the container, **electronic** content to expire on atime-dependent basis.974. A method of metering use of and/or access to**electronic** information characterized by the step of maint-ainin abitmap meter data structure including data partitions thatsubdivide the metering information by time and/or subjectmatter.146. A system for metering use of and/or access to**electronic** information characterized by means for maintaining abitmap meter data structure including data partitions thatsubdivide the metering information by time and/or subjectmatter.147. A distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, characterized in that the system permits at leastsome of the nodes to securely describe permitted uses of**electronic** content and securely enforces said description.148. In a distributed **electronic rights** management systemcomprising plural nodes having protected processingenvironments, a method characterized by the steps of permittingat least some of the nodes to securely describe permitted uses of**electronic** content, and securely enforcing said description.975. A document management system comprising one ormore **electronic** appliances containing one or more secureprocessing units and one or more secure databases operativelyconnected to at least one of said secure processing units... ...at least a portion of which usageinformation is reported to one or more parties.150. In a document management system comprising one ormore **electronic** appliances containin one or more secureprocessing units and one or more secure databases operativelyconnected to at least one of said secure processing units...information and the reportingof at least a portion of said usage information to one or moreparties.151. A document management system comprising plural**electronic** appliances containing protected processing976environments and one or more secure databases operativelyconnected to at least one of said protected processingenvironments, said system... ...and the reporting ofat least a portion of said usage information to one or moreparties.152. In a document management system comprising plural**electronic** appliances containing protected processingenvironments and one or more secure databases operativelyconnected to at least one of said protected processingenvironments, a method of... ...information, the production of usage information and thereporting of at least a portion of said usage information to one ormore parties.153. Am **electronic** contract system comprising **electronic**appliances containing one or more secure processing units andone or more secure databases operatively connected to at least977one of the secure processing units, said system furtheringincluding means for enabling plural parties to enter into an**electronic** arrangement, at least one of said databases contsecure control information for managing at least a portion of aplural party **electronic** arrangement.154. In an **electronic** contract system comprising plural**electronic** appliances containing one or more secure processingunits and one or more secure databases operatively connected toat least one of the secure processing units, a methodcharacterized by the steps of enabling plural parties

to enter intoto an **electronic** arrangement, and using secure controlinformation contained by at least one of said databases formanaging at least a portion of a plural party **electronic**arrangement.155. An **electronic** appliance arrangement containing atleast one secure processing unit and at least one secure databaseoperatively connected to at least one of said secure processing... ...atleast one aspect of appliance usage and control said usage basedat least in part upon protected appliance usage controlinformation.978. In an **electronic** appliance arrangement containing atleast one secure processing unit and at least one secure databaseoperatively connected to at least one of said secure processing information.157. An **electronic** appliance arrangement containing aprotected processing environment and at least one securedatabase operatively connected to said protected processingenvironment, said arrangement including means to... ...at least in part upon protected applianceusage control information processed at least in part through useof said protected processing environment.158. In an **electronic** appliance arrangement containing aprotected processing environment and at least one securedatabase operatively connected to said protected processingenvironment, a method characterized by the... ...based at least in part upon protected appliance usagecontrol information processed at least in part through use of saidprotected processing environment.979. An **electronic** appliance arrangement containing oneor more CPUs wherein at least one of the CPUs incorporates anintegrated secure processing unit, said arrangement storingprotected appliance usage control information designed to besecurely processed by said integrated secure processing unit.160. In an **electronic** appliance arrangement contone or more CPUs wherein at least one of the CPUs incorporatesan integrated secure processing unit, a method including the stepof storing and securely processing protected modular componentappliance usage control information with said integrated secureprocessing unit.161. An **electronic** appliance arrangement containing atleast one first secure processing unit and one or more videocontrollers where at least one of the video controllersincorporates... ...processing unit, saidarrangement storing protected video function control informationdesigned to be securely processed by said incorporated secureprocessing unit(s).162. In an **electronic** appliance arrangement containing atleast one first secure processing unit and one or more videocontrollers where at least one of the video controllersincorporates... ...characterized by the step of storing protected videofunction control information designed to be securely processed bysaid incorporated secure processing unit(s).163. An **electronic** appliance arrangement containing oneor more video controllers where at least one of the videocontrollers incorporates at least one secure processing unit, saidarrangement... ...control information is stored within a secure databaseoperatively connected to at least one of said at least one secureprocessing units.164. In an **electronic** appliance arrangement contone or more video controllers where at least one of the videocontrollers incorporates at least one secure processing unit, amethod... ...saidincorporated secure processing unit(s), within a databaseoperatively connected to at least one of said at least one secureprocessing units.165. An **electronic** appliance arrangement containing oneor more video controllers and ...control information is stored within a securedatabase operatively connected to at least one of said at least onesecure processing unit(s).166. An **electronic** appliance arrangement containing oneor more video controllers and at least one secure processing unit,a method including the step of storing component, modularprotected... ...secure processing unit(s), within asecure database operatively connected to at least one of said atleast one secure processing

unit(s).167. An **electronic** appliance arrangement containing atleast one secure processing unit and one or more networkcommunications means where at least one of the networkcommunications means... ...further secureprocessing unit, said arrangement storing protected networkingcontrol information designed to be processed bY said incorporatedsecure processing unit(s).168. In an **electronic** appliance arrangement containing atleast one secure processing unit and one or more network982communications means, a method characterized by the steps ofincorporating... ...in part within saidIncorporated secure processing unit(s), and securely processingsaid protected networking control information with said secureprocessing unit(s).169. An **electronic** appliance arrangement containing oneor more modems where at least one of the modems incorporatesat least one secure processing unit, said arrangement storingmodular, component protected modem control informationdesigned to be securely processed by said incorporated secureprocessing unit(s).170. In an **electronic** appliance arrangement contone or more modems where at least one of the modems. orporates at least one secure processing unit, a methodcharacterized by the step of storing and securely processingmodular, component protected modem control information withsaid incorporated secure processing unit(s).171. An **electronic** appliance arrangement containing atleast one secure processing unit and one or more modems whereat least one of the modems includes at least one... ...983processing unit, said arrangement storing protected modemcontrol information designed to be securely processed by saidincluded secure processing unit(s).172. In an **electronic** appliance arrangement containing atleast one secure processing unit and one or more modems whereat least one of the modems includes at least one... ...processing unit, a method including the step of storing andsecurely processing protected modem control information withinsaid included secure processing unit(s).173. An **electronic** appliance arrangement containing atleast one secure processing unit and one or more CD-ROMdevices where at least one of the CD-ROM devices said incorporated secure processing unit(s).174. In an **electronic** appliance arrangement containing atleast one secure processing unit and one or more CD-ROMdevices where at least one of the CD-ROM devices... ...method characterizedby the step of storing and securely processing protected CD-ROM984control information within said incorporated secure processingunit(s).175. An **electronic** appliance arrangement containing oneor more network communications means where at least one of thenetwork communications mean incorporates at least one secureprocessing unit, said arrangement storing modular, component,protected networking control information designed to be securelyprocessed by said incorporated secure processing unit(s).176. In an **electronic** appliance arrangement contone or more network communications means where at least oneof the network communications means incorporates at least onesecure processing unit... ...portion of saidcontrol information within said protected processingenvironment, and storing at least a portion of said controlinformation within said database.179. An **electronic** game arrangement containing aprotected processing environment for controlling the use of**electronic** games, said arrangement including game usage controlinformation, database means operatively connected to saidprotected processing environment for, at least in part, storingusage control... ...for regulating at least some aspect ofuse of at least a portion of at least one of said games, andtraveling objects containing protected **electronic** game content.180. In an **electronic** game arrangement

containing aprotected processing environment for controffing the use of**electronic** games, a method including the steps of(a) including game usage control information within adatabase means operatively connected to said protectedprocessing environment; and...

...least one of said games.181. A method as in claim 178 further including the step ofregulating the use of traveling objects containing protected**electronic** game content.182. An **electronic** game arrangement containinginteroperable protected processing environments for controllingthe use of interactive games, said arrangement includingprotected game usage control information, and database meansoperatively connected to said protected processing environmentsfor, at least in part, storing game usage control information.183. In an **electronic** game arrangement containingprotected processing environments, a method comprising:(a) storing, within a secure database mean operativelyconnected to said protected processing environments protectedgame usage control information; and(b) controlling the use of interactive games based at leastin part on the storing game usage control information.184. An **electronic** game arrangement containinginteroperable protected processing environments for controlling987the use of games, said arrangement including component,modular, protected game usage control information, wherein atleast a portion of said protected control information was providedindependently by plural parties securing their respective **rights**in at least one **electronic** value chain.185. In an **electronic** game arrangement continteroperable protected processing environments for controllingthe use of games, a method including the steps of(a) providing at least a portion of component, modular,protected game usage control information independently byplural parties; and(b) using the control information at least in part tosecuring respective **rights** of said plural parties in at least one**electronic** value chain.186. An **electronic** multimedia arrangement contprotected processing environments for controlling the use ofmultimedia, said arrangement including component, modularmultimedia usage control information and database meansoperatively connected to said protected processing environmentsfor, at least in part, storing multimedia usage controlinformation.988. In an **electronic** multimedia arrangement cont 0 iprotected processing environments for controlling the use ofmultimedia, a method including the steps of storing multimediausage control information within a database means operativelyconnected to said protected processing environments, and usingthe stored control information to control multimedia.188. An **electronic** multimedia arrangement containing aprotected processing environment for controlling the use ofmultimedia, said arrangement including multimedia usagecontrol information, database means operatively connected tosaid protected processing environment for, at least in part,storing multimedia usage control information, and protectedtraveling objects containing distributed multimedia **electronic**content.189. In an **electronic** multimedia arrangement containinga protected processing environment, a method characterized bythe steps of storing multimedia usage control information withina database mean operatively connected to said protectedprocessing environment, and controlling, based at least in part onthe stored information, protected traveling objects containingdistributed multimedia **electronic** content.989. An **electronic** multimedia arrangement cont 6 ointeroperable protected processing environments for controllingthe use of multimedia, said arrangement including component,modular, protected multimedia usage control information,wherein at least a portion of said protected control informationwas provided independently by plural parties securing theirrespective **rights**

in at least one **electronic** value chain.191. A system as in claim 188 further including a secureprocessing unit.192. In an electro
nic multimedia arrangement cont
protected processing environments, a method comprisingproviding at least a portion of component, modular, protectedmultimedia usage control information independently by pluralparties securing their respective **rights** in at least one **electronic**value chain, and using the ...software.197. An integrated circuit comprising at least onemicroprocessor, memory, input/output means, a tamper resistantbarrier and at least a portion of a **Rights** Operating System.198. An integrated circuit comprising at least onemicroprocessor, memory, input/output means, at least one real991time clock, a tamper resistant...
...second secure event processing environmentinteroperable with the first event processing environment formanaging the processing of such an event.203. A method for enabling **electronic** commerce chain ofhandling and control characterized by the step of a first and asecond party independently specifying protected, modularcomponent control information describing requirements relatedto the operation of an **electronic** commerce value ch i .204. A system for enabling **electronic** commerce chain ofhandling and control characterized by means for permitting afirst and a second party to independently specify protected,modular component control information describing requirementsrelated to the operation of an **electronic** commerce value chain ofhandling and control, and means for securely enforcing therequirements described by the control information.993. A method for enabling **electronic** commercecharacterized by the step of a first and a second partyindependently stipulating control information managing the useof **digital** information, wherein said first and said second partyindependently maintain persistent lights enforced by said controlinformation as said **digital** information moves through a chain ofhandling and control.206. A system for enabling **electronic** commerce including:means for allowing a first party to stipulate controlinformation managing the use of **digital** information,means for allowing a second party to stipulate controlinformation managing the use of the **digital** information, andchain of handling and control means for maint i ipersistent **rights** enforced by said control information as said**digital** information moves from one location and/or process toanother.207. A method for secure maintenance of **electronic rights**comprising a first step of plural parties in a value chainindependently and securely stipulating control informationregarding their **electronic rights**, wherein said controlinformation is used to enforce conditions related to the use of**electronic** information distributed in software containers.994. A system for secure maintenance of **electronic rights**comprising:means permitting plural parties in a value chain toindependently and securely stipulates control informationregarding their **electronic rights**, andmeans for using said control information to enforceconditions related to the use of **electronic** information distributedin software containers.209. A method for securely controlling the use of protected**electronic** content including the step of supporting modularseparate control information arrangements for managing at leastone event related to use of said content such that... ...user mayselect between separate control information arrangements formanaging such at least one event.210. A system for securely controlling the use of protected**electronic** content including modular separate controlinformation arrangements for managing at least one eventrelated to use of said content such that a user may select... ...separate control information arrangements for managing such atleast one event.211. A method employing separate, modular

controlstructures for managing the use of encrypted **digital** information995characterized by the step of enabling commercial value chainparticipants to support plural relationships between two or moreof. (1) content event triggering, (2) auditing, and (3) budgeting,control variables.212. A system for employing separate, modular controlstructures for managing the use of encrypted **digital** informationcharacterized by means for enabling commercial value chainparticipants to support plural relationships between two or moreof. (1) content event triggering, (2) auditing, and (3) budgeting,control variables.213. A method of chain of handling and control enabling aparty not directly participating in an **electronic** value chain tocontribute secure control information to enforce at least onecontrol requirement, said method characterized by a first step ofa first value chain participant stipulating control informationassociated with **digital** information and a second step whereinsaid not directly participating party independently and securelycontributes secure control information for inclusion in anaggregate control information... ...said associatedcontrol information, said aggregate control information at least inpart managing conditions related to the use of at least a portionof said **digital** information by a second value chain participant.996. A chain of handling and control system for enabling aparty not directly participating in an **electronic** value chain tocontribute secure control information to enforce at least onecontrol requirement, said system characterized by:means for allowing a first value chain participant tostipulate control information associated with **digital** information,means for allowing the not directly participating party toindependently and securely contribute secure control informationfor inclusion in an aggregate control information set... ...means responsive to said aggregate controlinformation for at least in part managing conditions related tothe use of at least a portion of said **digital** information by asecond value chain participant.215. A method of **electronic** commerce control informationmanagement for delegating the admini tration of certain **rights**held by a value chain party to a second value chain partycharacterized by the step of said first party stipulating securecontrol information describing at least a portion of -their **rights**related to one or more chain of handling and control **electronic**events wherein said first party provides further controlinformation authorizing said second party to admini ter some orall of said **rights** as an agent for said first party.997. A system for **electronic** commerce control informationmanagement for delegating the administration of certain **rights**held by a value chain party to a second value chain partycharacterized by:means for allowing said first party to stipulate securecontrol information describing at least a portion of their **rights**related to one or more chain of handling and control **electronic**events; andmeans for allowing said first party to provide finwthercontrol information authorizing said second party to admini tersome or all of said **rights** as an agent for said first party.217. A method of governing taxation of commercial eventsresulting from **electronic** chain of handling and controlcharacterized by a first step of distributing secure **digital**information to a user and specifying secure control informationcontrolling at least one condition for use of said **digital**information and a second step of a government agency securely,independently contributing secure control information forautomatically governing tax payments for said commercialevents.218. A system for governing taxation of commercial eventsresulting from **electronic** chain of handling and controlcharacterized by:998means for distributing secure **digital** information to a user;means for specifying secure control information controllingat least one condition for

use of said **digital** information; andmeans for ...a government agency to securely,independently contribute secure control information forautomatically governing tax payments for said commercialevents.219. A method of governing privacy **rights** related to**electronic** events characterized by a first step of a first partyprotecting **digital** information containing information descriptiveof preventing a second party from at least one unauthorized useand a second step of specifijing certain control informationrelated to use of at least a portion of said protected **digital**information, wherein said control information enforces at leastone **right** of said second party related to privacy and/or permitteduse(s) of personal and/or proprietary information included in saidprotected **digital** information.220. A system for governing privacy **rights** related to**electronic** events characterized by:means for permitting a first party to protect **digital**information containing information descriptive of preventing asecond party from at least one unauthorized use;999means for specifying certain control information related touse of at least a portion of said protected **digital** information; andmeans for using the control information to enforce at leastone **right** of said second party related to privacy and/or permitteduse(s) of personal and/or proprietary information included in Saidprotected **digital** information.221. A method of governing privacy **rights** related to**electronic** events characterized by a first step of a first partyprotecting **digital** information from at least one unauthorized useand stipulating certain control information for establishingconditions for use of said protected information and a second stepof a user of said **digital** information stipulating further controlinformation regulating the reporting of information regardingsaid user's use of at least a portion of said **digital** information.222. A system for governing privacy **rights** related to**electronic** events characterized by:means for allowing a first party to protect **digital**information from at least one unauthorized use and forstipulating certain control information for establishing conditionsfor use of said protected information; andmeans for allowing a user of said **digital** information tostipulate fin-ther control information regulating the reporting of1000information regarding said user's use of at least a portion of said**digital** information.223. A secure method for regulating **electronic** conduct andcommerce characterized by a step of distributing interoperableprotected processing environments and circulating amongstplural recipients of said protected processing environmentssoftware containers containing **digital** content and relatedcontent control information prepared for use by at least a portionof said protected processing environments, wherein said methodincludes the further step of regulating the use at least some ofsaid **digital** content based, at least in part, on the secureprocessing of at least a portion of said control informationthrough the use of at least one protected processing environment.224. A secure system for regulating **electronic** conduct andcommerce characterized by:distributed interoperable protected processingenvironments,means for circulating, amongst said protected processingenvironments, software containers containing **digital** content andrelated content control information prepared for use ...of said protected processing environments, andmeans within at least some of the protected processingenvironments for regulating the use at least some of said **digital**1001content based, at least in part, on the secure processing of atleast a portion of said control information.225. A method of **electronic** commerce networking forenabling a secure **electronic** retail environment characterized bythe step of supplying user certified control information, smartcards, secure processing units, and retailing terminalarrangements

networked together using VDE communicationtechniques and secure software containers.226. An **electronic** commerce networking system forenabling a secure **electronic** retail environment characterized by:means for networking together smart cards, secureprocessing units, and retailing terminal arrangements; andmeans for making the smart cards, secure processing units,and retailing terminal arrangements interoperable with oneanother and with VDE communication techniques and securesoftware containers.227. A method of enabling **electronic** commerce appliancesfor securely administering user **rights** in commerce activitiescharacterized by the step of providing to users at least a portionof a VDE node contained within a physical device, said... ...be compatible with mating connectors in host1002systems for supporting secure, interoperable transaction activitybetween plural parties.228. A system for securely administering user **rights** incommerce activities comprising a physical device including atleast a portion of a portable VDE node, said device beingconfigured to be compatible with mating connectors in hostsystems for supporting secure, interoperable tran action activitybetween plural parties.229. A method for enabling a programme le, **electronic**commerce environment characterized by the step of providing tomultiple parties secure commerce nodes that securely processseparate, modular component billing management methods,budgeting management... ...methods, and related auditing management methods and furthercharacterized by the step of supporting triggering of metering,auditing, billing, and budgeting methods in response to **electronic**commerce event activities.230. A programmable, **electronic** commerce environmentcharacterized by secure commerce nodes each including:means for securely processing separate, modularcomponent billing management methods, budgeting management1003methods, metering management methods, and related auditingmanagement methods, andmeans for supporting triggering of metering, auditing,billing, and budgeting methods in response to **electronic**commerce event activities.23 1. An **electronic** com-rn erce system including modular,standardized control components comprising **electronic** commerceevent control instructions stipulated by commerce participants,and plural **electronic** appliances containing one or more secureprocessing units which process at least a portion of suchcommerce event control instructions, said system furthercontaining one... ...in partsecurely storing at least a portion of such control instructions foruse by said at least one secure processing unit.232. In an **electronic** commerce system including modular,standardized control components comprising **electronic** commerceevent control instructions stipulated by commerce participants,and plural **electronic** appliances containing one or more secureprocessing units which ...atleast a portion of such control instructions for use by said at leastone secure processing unit.233. A content distribution system comprising plural**electronic** appliances containin one or more interoperable secureprocessing units operatively connected to one or more databasesfor use with at least one of said secure processing units, said oneor more databases containing (a) one or more decryption keys foruse in decrypting distributed, encrypted **digital** information, and(b) encrypted audit information, said audit information reflectingat least one aspect of use of said distributed **digital** information234. A content distribution method comprising:distributing plural **electronic** appliances containing one ormore interoperable secure processing unitsoperatively connecting the appliances to one or moredatabases,storing within said one or more databases one or moredecryption keys,using the decryption keys for decrypting distributed,encrypted **digital** information,

andstoring within the one or more databases encrypted auditinformation, said audit information reflecting at least one aspectof use of said distributed **digital** information.1005. An **electronic** currency system comprising plural,**electronic** appliances containing (a) protected processienvironments, (b) encrypted **electronic** currency and relatedsecure control information configured so as to be useable by atleast one of said protected processing environments, and (c)usage reporting means for securely communicating **electronic**currency usage related information from a first interoperableprotected processing environment to a second interoperableprotected processing environment.236. An **electronic** currency method comprising:distributing plural, **electronic** appliances containing (a)protected processing environments, (b) encrypted electro .currency and related secure control information configured so asto be useable by at least one of said protected processingenvironments, andsecurely communicating **electronic** currency usage relatedinformation from a first interoperable protected processingenvironment to a second interoperable protected processingenvironment.237. A method for **electronic** financial activitiescharacterized by the steps of1006communicating **digital** containers cont i 0financial information from a first interoperablesecure node to a second interoperable secure node,communicating modular, standard controlinformation to said... ...of at least a portion ofsaid financial information,reporting information related to said use to said firstinteroperable secure node.238. A system for **electronic** financial activitiescharacterized by:mean for communicating **digital** containers containinfinancial information from a first interoperable secure node to asecond interoperable secure node,means for communicating modular, standard controlinformation to said 239. A method for **electronic** currency managementincluding:1007communicating encrypted **electronic** currency from a first,interoperable secure user node to a second interoperable usernode using at least one secure container, andproviding secure control information... ...with said atleast one secure container, said secure control information, atleast in part, maintainin conditionally anonymous currencyusage information.240. A system for **electronic** currency managementincluding:means for communicating encrypted **electronic** currencyfrom a first, interoperable secure user node to a secondinteroperable user node using at least one secure container, andmeans for providing secure... ...said at least one secure container, said secure controlinformation, at least in part, maintaining conditionallyanonymous currency usage information.24 1. A method for **electronic** financial activitiesmanagement characterized by the steps ofsecurely communicating from a first secure node to asecond secure node financial information standardized controlinformation... ...wherein saidstandardized control information is at least in part stored in asecure database contained within said third secure node.242. A system for **electronic** financial activitiesmanagement characterized by the steps of:means coupled-to a first and a second secure node forsecurely communicating from said first secure...executable content in accordance with at least aportion of at least one of said at least one associated rule and/orcontrol.247. A **rights** distributed database environment including(a) means allowing one or more central authorities to establishcontrol information for use of encrypted **digital** information, (b)interoperable database management systems at plural user sitesfor securely storing control information and audit information, (c)secure communication means for securely communicating... ...information and audit information between user sites, and (d)centralized database mean

for compiling and analyzing usageinformation from plural user sites.248. Within a **rights** distributed database environment, amethod characterized by the following steps:establishing control information for use of encrypted **digital**information,securely storing, within interoperable databasemanagement systems at plural user sites, control informationand audit information,securely communicating control information and auditinformation between...with the search results for establishing at least one conditionrelated to the use of at least one portion of said search results.253. A **rights** management system comprising protectedinformation, at least two protected processing arrangements, anda **rights** management language that allows the expression ofpermitted operations and the consequences of performing suchoperations on at least a portion of the information processed atleast in part by at least one of the protected processingarrangements.1014. A **rights** management method comprising:providing protected information for processing by at leasttwo protected processing arrangements, andexpressing, in a **rights** management language, permittedoperations and the consequences of performing such operationson at least a portion of the information processed at least in partby at least one of the protected processing arrangements.255. A method of protecting **digital** informationcharacterized by the steps of encrypting at least a portion of theinformation, using a **rights** management language to describe theconditions related to use of the information, distributing at leasta portion of such information and at least a portion of such **rights**language expressed conditions to one or more recipients, using an**electronic** appliance arrangement including at least one protectedprocessing arrangement to securely govern at least a portion ofthe use of such information.256. A system for protecting **digital** informationcharacterized by:mean for encrypting at least a portion of the information,mean for using a **rights** management language to describethe conditions related to use of the information,1015means for distributing at least a portion of suchinformation and at least a portion of such **rights** languageexpressed conditions to one or more recipients, andan **electronic** appliance arrangement including at least oneprotected processing arrangement for securely governing at leasta portion of the use of such information.257. A distributed **digital** information management systemcomprising software components, a **rights** management languagefor expressing processing relationships between two or more ofthe software components, protected processing means for at leasta portion of the software components and at least a portion of the**rights** management expressions, means for protecting content,means for creating software objects that relate protected contentto **rights** management expressions, and means for deliveringprotected content, **rights** management expressions, and suchsoftware objects from a providing location to a user's location.258. A distributed **digital** information managementmethod comprising:expressing, in a **rights** management language, processingrelationships between two or more of the software components,processing, within at least one protected environment, atleast a portion of the software components and at least a portionof the **rights** management expres

sions,
1016protecting content,creating software objects that relate protected content to**rights** management expressions, anddelivering protected content, **rights** managementexpressions, and such software objects from a providing locationto a user's location.259. An authentication system comprising at least two**electronic** appliances, at least two **digital** certificates reflectingidentity information encrypted using different

certifying privatekeys where such certificates are stored in a first **electronic**appliance, communications mean for transmitting and receivingsignals between **electronic** appliances, means for determiningcompromised and/or expired certifying private keys operativelyconnected to a second **electronic** appliance, mean for the second**electronic** appliance to request transmission of one of the **digital**certificates from the first **electronic** appliance based at least inpart on such determination, and mean operatively connected tosuch second **electronic** appliance for decrypting such certificateand determining such certificate's validity and/or the validity ofidentity information.260. In a system comprising at least two **electronic**appliances, an authenticating method comprising:1017issuing at least two **digital** certificates reflectingidentification information, including the step of encrypting thetwo certificates using different certifying private keys,storing the certificates in a first **electronic** appliance,transmitting and receiving signals between electroappliances,determining compromised and/or expired certifying privatekeys operatively connected to a second **electronic** appliance,requesting, with the second **electronic** appliance,transmission of one of the **digital** certificates from the first**electronic** appliance based at least in part on such determination,decrypting such certificate with the second **electronic**appliance, anddetermining such certificate's validity and/or the validity ofidentity information.261. An authentication system comprising at least two**electronic** appliances, at least two **digital** certificates reflectingidentify information encrypted using different certifying privatekeys where such certificates are stored in a first **electronic**appliance, communications means for transmitting and receivingsignals between **electronic** appliances, means for a second**electronic** appliance to request transmission of one of the **digital**certificates from the first **electronic** appliance wherein theselection of which certificate is requested is based at least in part1018on a random or pseudo-random number, means operativelyconnected to such second **electronic** appliance for decrypting suchcertificate and determining such certificate's validity and/or thevalidity of identity information.262. In a system comprising at least two **electronic**appliances, an authenticating method comprising:issuing at least two **digital** certificates reflecting identifyinformation, including the step of encrypting the two **digital**certificates using different certifying private keys,storing such certificates in a first **electronic** appliance,tran mitting and receiving signals between **electronic**appliances,requesting, with a second **electronic** appliance,transmission of one of the **digital** certificates from the first**electronic** appliance, including the step of selecting a certificatebased at least in part on a random or pseudo-random number,decrypting such certificate with the second **electronic**appliance; anddetermining such certificate's validity and/or the validity ofidentity information.263. A method of secure **electronic** mail characterized bythe steps of creating at least one **electronic** message using aninteroperable protected processing environment, encrypting at1019least a portion of said at least one message, securely associatingone or more sets... ...control information with one or moremessages to set at least one condition for the use of said at leastone message, communicating the protected **electronic** messages toone or more recipients having protected processing environments,securely communicating at least one set of the same or differingcontrol information to each... ...protected messages to use messageinformation at least in part in accordance with the conditionsspecified by the control information.264. A system for secure **electronic** mail including multipleprotected processing environments, the system characterized by:a first protected processing

environment for creating atleast one **electronic** message, the first environment includingmean for encrypting at least a portion of said at least onemessage, means for securely associating one or more... ...one or more messages to set at least onecondition for the use of said at least one message, and means forcommunicating the protected **electronic** messages to one or morerecipients having interoperable protected processingenvironments,means for securely communicating at least one set of thesame or differing control...andmeans for delivering the new enabling control informationand/or protected information to a second user.267. A method of controlling redistribution of distributed**digital** information including the steps of encrypting **digital**information, distributing said encrypted **digital** information froma first party to a second party, establishing control informationregarding the redistribution of at least a portion of said encrypted**digital** information from said second party to at least one third1022party, regulating the redistribution of said at least a portion ofsaid encrypted **digital** information through the use of a protectedprocessing environment processing said control information.268. A system for controlling redistfibution of distributed**digital** information including:men-n for encrypting **digital** information,meanis for distributing said encrypted **digital** informationfrom a first party to at least one second party,means for establishing control information regarding theredistribution of at least a portion of said encrypted **digital**information from said second party to at least one third party,anda protected processing environment for processing saidcontrol information and for regulating the redistribution of saidat least a portion of said encrypted **digital** information.269. A method of controlling a robot characterized by thesteps of creating instructions for one or more robots, creating asecure container incorporating...which such instructions may beused and the nature of audit reports required when suchinstructions are performed.273. A method of detecting fraud in **electronic** commercecharacterized bv the steps of creating at least one secure1024container, associating control information with such one or morecontainers including control information... ...control information,detecting cases where certain audit information differs at least inpart from such profile of usage.274. A system for detecting fraud in **electronic** commercecharacterized bymeans for creating at least one secure container,means for associating control information with such one ormore containers including control information... ...mean for detecting cases where certain audit informationdiffers at least in part from such proffie of usage.275. A method of detecting fraud in **electronic** commercecharacterized by the steps of distributing at least in partprotected **digital** information to customers7 distributing one ormore **rights** to use at least a portion of such **digital** informationacross an **electronic** network, allowing a customer to use at leasta part of said at least in part protected **digital** informationthrough the use of a protected processing environment and atleast one of said one or more distributed **rights**, detectingunusual usage activity related to use of said **digital** information.276. A system for detecting fraud in **electronic** commercecharacterized bymeans for distributing at least in part protected **digital**information to customers,means for distributing one or more **rights** to use at least aportion of such **digital** information across an **electronic** network,a protected processing environment for allowing acustomer to use at least a part of said at least in part protected1026**digital** information through at least one of said one or moredistributed **rights**, andmeans for detecting unusual usage activity related to useof said **digital** information.277. A programmable component arrangement comprisinga tamper resistant processing environment including

amicroprocessor, memory, a task manager, memory manager andexternal interface controller... ...with such created components,andsecurely delivering such created components between atleast two of said at least two tamper resistant processingenvironments.281. An **electronic** appliance comprising at least one CPU,memory, at least one system bus, at least one protectedprocessing environment, and at least one of a **Rights** OperatingSystem or **Rights** Operating System layer associated with a hostoperating system.282. An operating system comprising at least one taskmanager. at least one memory manager, at least one input/outputmanager, at least one protected processing environment, mean1029for detecting events, means for associating events with **rights**control functions, means for performing **rights** control functions ...least one memory manager, at least one input/outputmanager, at least one protected processing environment, anoperating method comprising:detecting events,associating events with **rights** control fimctions, andperforming **rights** control fimctions at least in part withinsuch one or more protected processing environments.284. A method of business automation characterized bythe steps of...with said data item.321. A method for securely managing at least oneoperation on a data item performed at least in part by an**electronic** arrangement, said method comprising:(a) securely delivering a first procedure to said **electronic**arrangement;(b) securely delivering, to said **electronic** arrangement, asecond procedure separable or separate from said first procedure;W performing at least one operation on said data item,including using said first...said deliveringstep (a) includes:encrypting at least a portion of said first procedure,communicating said at least in part encrypted firstprocedure to said **electronic** arrangement,decr-ypting at least a portion of said first procedure at leastin part using said **electronic** arrangement, andvalidating said first procedure with said **electronic**arrangement.1046. A method as in claim 319 wherein said deliveringstep (b) includes delivering at least one of said first and secondprocedures within... ...wherein said performingstep includes budgeting usage.341. A method for securely managing at least oneoperation performed at least in part by a secure **electronic**appliance, comprising:(a) selecting an item that is protected with respect to atleast one operation;(b) securely independently delivering plural separateprocedures to said **electronic** appliance;1047(c) using said plural separate procedures in combination toat least in part securely manage said operation with respect tosaid selected item... ...340 wherein said performingstep includes budgeting usage.349. A method as in claim 340 wherein said performingstep includes electronically processing content based on **electronic**controls.350. A method of securely controlling at least oneprotected operation with respect to a data item comprising:(a) supplying at least a first...dynamicall negotiating between said first and secondycontrols.361. A method as in claim 358 wherein said controllingstep (b) includes controlling decryption of **electronic** content.362. A method as in claim 358 further including:receiving protected **electronic** content from a party; andauthenticating the identity of said party prior to using saidreceived protected **electronic** content.1052. A secure method comprising:selecting protected data;extracting said protected data from an object;identffying at least one control to manage at least... ...modules; andsecurely applying said first and second load modules tomanage said resource for use with said data item.370. A method for negotiating **electronic** contracts,comprising:receiving a first control set from a remote site;providing a second control set;performing, within a protected processing environment, an**electronic** negotiation between said first control set and said1054second

control set, including providing interaction between saidfirst and second control sets; andproducing a negotiated control set resulting from saidinteraction between said first and second control sets.371. A system for supporting **electronic** commerceincluding:means for creating a first secure control set at a firstlocation;means for creating a second secure control set at a second... ...second location for securely integrating saidfirst and second control sets to produce at least a third control setcomprising plural elements together comprising an **electronic**value chain extended agreement.372. A system for supporting **electronic** commerceincluding:means for creating a first secure control set at a firstlocation;means for creating a second secure control set at a second... ...securely communicating said first secure controlset from said first location to said second location; andnegotiation means at said second location for negotiatingan **electronic** contract through secure execution of at least aportion of said first and second secure control sets.373. A ...controls, and(b) securely applies said first and second controls tomanage said resource for use of said data item.381. A system for negotiating **electronic** contracts,comprising:a storage arrangement that stores a first control setreceived from a remote site, and stores a second control set;a protected processing environment, coupled to saidstorage arrangement, that:(a) performs an **electronic** negotiation between saidfirst control set and said second control set,(b) provides interaction between said first andsecond control sets, and(c) produces a... ...claim 379 further including mean forelectronically enforcing said negotiated control set.383. A system as in claim 379 further including means forgenerating an **electronic** contract based on said negotiated controlset.384. A method for supporting **electronic** commerceincluding:creating a first secure control set at a first location;creating a second secure control set;electronically negotiating, at said location different fromsaid first location, an **electronic** contract, including the step ofsecurely executing at least a portion of said first and secondcontrol sets.385. An **electronic** appliance comprising:a processor; andat least one memory device connected to said processor;wherein said processor includes:retrieving means for retrieving at least one... ...and1060using means coupled to said retrieving means for usingsaid component to form said component assembly in accordancewith said record.386. An **electronic** appliance comprising:at least one processor;at least one memory device connected to said processor;andat least one input/output connection operatively coupled tosaid processor,wherein said processor at least in part executes a **rights**operating system to provide a secure operating environmentwithin said **electronic** appliance.387. An **electronic** appliance as in claim 384 wherein saidprocessor includes mean for providing a channel, said channelassembling independently deliverable components into acomponent assembly and executing said component assembly.388. An **electronic** appliance as in claim 384 furtherincluding a secondary storage device coupled to said processor,said secondary storage device storing a secure database, saidprocessor including means for decrypting information obtainedfrom said secure database and for encrypting information to bewritten to said secure database.1061. An **electronic** appliance as in claim 384 wherein saidprocessor and said memory device are disposed in a secure,tamper-resistance encapsulation.390. An **electronic** appliance as in claim 384 wherein saidprocessor includes a hardware encryptor/decryptor.391. An **electronic** appliance as in claim 384 wherein saidprocessor includes a real time clock.392. An **electronic** appliance as in claim 384 wherein saidprocessor includes a random number generator.393. An **electronic**

appliance as in claim 384 wherein saidmemory device stores audit information.394. A method for auditing the use of at least one resourcewith... ...second auditinformation being at least in part different from said first auditinformation.1063. A method and/or system for enabling asale ofprotected **digital** information that has been previously distributedto users, the method or system being characterized by a secureelement that selectively controls access to the protected **digital**information based on **electronic** controls associated with theinformation.397. A distributed, secure **electronic** point of sale system ormethod characterized by a secure processing element forselectively releasing goods and/or services in exchange forcompensation.398. In a distributed **digital** network, an advertisingmethod characterized by the steps of tracking usage of **digital**information that has associated with it one or more controls withrespect to access to and/or usage of said information; andtargeting advertising messages based at least in part on saidtracking.399. A distributed **electronic** advertising systemcharacterized in that the system uses a distributed network ofinteroperable protected processing environments to at least inpart deliver advertising to users...or auditing.40 1. A protected processing system or method providingmultiple currencies and/or payment arrangements for the secureprocessing and releasing of protected **digital** information.402. A distributed secure method or system characterizedin that a user's age is used as a criteria for electronically,securely releasing information and/or resources to the user.403. A method of renting an **electronic** appliance defininga secure processing environment.404. A virtual distribution environment providing any oneor more of the following features and/or elements and/or... ...pathways for providing information, for controlinformation, and/or for reporting; and/ormultiple payment methods; and/ormultiple currencies; and/orEDI; and/or**Electronic** banking; and/or**electronic** document management; and/or**electronic** secure communication; and/ore-mail; and/ordistributed asynchronous reporting; and/orcombination asynchronous and **online** management; and/orprivacy control by users; and/ortesting; and/orusing age as a class; and/orappliance control (renting, etc.); and/ortelecommunications infrastructure; and/orgames management; and/orextraction of content from an **electronic** container; and/orembedding of content into an **electronic** container; and/ormultiple certificate to allow for breach of a key; and/orvirtual black box; and/or1066independence of control information from content; and/ormultiple, separate, simultaneous control sets for one **digital**information property; and/orupdating control information for already distributed **digital**information; and/ororganization information management; and/orcoupled external and organization internal chain ofhandling and control; and/ora content usage consequence management system(reporting, payment, etc., multiple directions); and/ora content usage reporting system providing differing auditinformation and/or reduction going to multiple parties holding**rights** in content; and/oran automated remote secure object creation system; and/orinfrastructure background analysis to identify improperuse; and/orseniority of control... ...system; and/orsecure distribution and enforcement of rules and controlsseparately from the content they apply to; and/orredistribution management by controlling the **rights** and/ornumber of copies and or pieces etc. that may be redistributed;and/oran **electronic** commerce taxation system; and/oran **electronic** shopping system; and/oran **electronic** catalog system; and/or1067a system handling **electronic** banking, **electronic** shopping,and **electronic** content usage management; and/oran **electronic** commerce multimedia system; and/ora distributed, secure, **electronic**

point of sale system; and/oradvertising; and/orelectronics **rights** management; and/ora distributed **electronic** commerce system; and/ora distributed transaction system or environment; and/ora distributed event management system; and/ora distributed **right** systems.405. A Virtual Distribution Environment substantially asshown in Figure 1.406. An "Information Utility" substantially as shown inFigure 1A.407. A chain...4,411. An object substantially as shown in Figures 5A and5B.412. A Secure Processing Unit substantially as shown inFigure 6.413. An **electronic** appliance substantially as shown inFigure 7.414. An **electronic** appliance substantially as shown inFigure 8.415. A Secure Processing Unit substantially as shown inFigure 9.416. A 'Rights Operating System" ("ROS") architecturesubstantially as shown in Figure 10.417. Functional relationship(s) between applications andthe **Rights** Operating System substantially as shown in Figures11A-11C.1069. Components and component assemblies substantiallyas shown in Figures 11D-11J.419. A **Rights** Operating System substantially as shown inFIGURE 12.420. A method of objection creation substantially as shownin Figure 12A.421. A "protected processing environment... ...event log substantially as shownin FIGURE 29.440. A method of interrelating and using an objectregistration table, a subject table and a user **rights** tablesubstantially as shown in Figure 30.441. A method of using a site record table and a grouprecord table to track portions of...as shown in FIGURE 68.466. A process of downloading firmware into a protectedprocessing environment substantiaRy as shown in FIGURE 69.1075. Multiple VDE **electronic** appliances conn cted together witha network or other communications means substantially asshown in FIGURE 70.468.A portable VDE **electronic** appliance substantially asshown in FIGURE 71.469. Pop-up " displays that may be generated by the usernotification and exception interface substantially as shown... ...72D. 470. A smart object substantially as shown in FIGURE 73.471. A method of processing smart objects substantially asshown in FIGURE 74.472. **Electronic** negotiation substantially as shown in anyof FIGURES 75A-75D.473. An **electronic** agreement substantially as shown inFIGURES 75E-75F.474. **Electronic** negotiation processes substantially asshown in any of FIGURES 76A-76B.1076. A chain of handling and control substantially asshown in FIGURE 77.476...leastin part, the control information.484. A business automation system comprising (a)distributed, interoperable protected processing environmentinstallations, (b) secure containers for distribution of **digital**1078information, (c) control information supporting the automation ofchain of handling and control fianctions.485. A method of business automation characterized bythe steps of providing interoperable protected processingenvironment nodes to plural parties, communicating firstencrypted **digital** information from a first party to a second party,communicating second encrypted **digital** information including atleast a portion of said first communicated **digital** informationand/or information related to the use of said first **digital**information, to a third party different from said first or secondparties, wherein use of said second encrypted **digital** informationis regulated, at least in part, by an interoperable protectedprocessing environment available to said third party.486. A business automation system characterized by:plural protected processing environment nodes,means for communicating **digital** information between thenodes, andwherein at least one of the nodes includes means forregulating the use of said communicated **digital** information.487. A method for chain of handling and controlcharacterized by the steps of (a) a first party placing protected**digital** information into a first software container and stipulating1079rules and controls governing use of at

least a portion of said**digital** information, (b) providing said software container to asecond party, wherein said second party places said softwarecontainer into a further software container and stipulates rulesand controls for at least in part managing use of at least a portionof said **digital** information and/or said first software container bya third party.488. A chain of handling and control system characterizedby:means for placing **digital** information into a first softwarecontainer and for stipulating rules and/or controls governing useof at least a portion of said **digital** information, andmeans for placing said ...software container and for stipulating fin-ther rules and/orcontrols for at least in part managing use of at least a portion ofsaid **digital** information and/or said first software container.489. A system for chain of handling and control including(a) a first container containing at least in part protected **digital**information, (b) at least in part protected control informationstipulated by a first party establishing conditions for use of atleast a portion of said **digital** content, (c) a second containerdifferent from said first container, said second containercontaining said first container, (d) control information stipulated1080independently by a second party for at least in part settingconditions for managing use of the contents of said secondcontainer.490. A system for **electronic** advertising including: (a)means to provide **digital** information to users for their use, (b)means to provide advertising content to said users incombination with said **digital** information, (c) means to audit useof said **digital** information, (d) means to securely acquire usageinformation regarding use of advertising content, (e) means tosecurely report information based upon said advertising contentusage information, (f) compensating at least one content providerat least in part based upon use of said advertising content.491. A method for **electronic** advertising characterized bythe steps of (a) placing **digital** information into a container, (b)associating advertising information with at least a portion of said**digital** information, (c) securely providing said container to acontainer user, (d) monitoring user viewing of advertisinginformation, and (d) receiving payment from an advertiser,wherein said payment is related to user viewing of saidadvertising information.492. A system for **electronic** advertising involving (a)means to containerize **digital** information including both content1081and advertising information, (b) means to monitor viewing of atleast a portion of said advertising information, (c) mean to... ...said advertisinginformation, (d) means to securely communicate informationbased upon said viewing in a secure container, and (e) controlinformation related to said containerized **digital** information formanaging the communication of said information based uponsaid viewing.493. A method for **electronic** advertising characterized bythe steps of (a) containerizing **digital** information including bothcontent and advertising information, (b) monitoring user viewingof at least a portion of said advertising information, (c) chargingfor user viewing... ...advertising information, the communication of information basedupon said viewing.494. A method of clearing transaction informationcharacterized by the steps of (a) securely distributing **digital**information to a first user of an interoperable protectedprocessing environment, (b) securely distributing further **digital**information to a user of an interoperable protected processing1082environment different from said at first user W receivinginformation related to usage of said **digital** information, (d)receiving information related to usage of said further **digital**information, and (e) processing information received according tosteps (c) and (d) to perform at least one of (I) an admini trative,or (II) an analysis, function.495. A system for clearing transaction informationincluding (a) a first container containing at

least in partprotected **digital** information and associated control information,(b) a second secure container containing further at least in partprotected **digital** information and associated control information,W means to distribute said first and second containers to users,(d) communication means for communicating information at leastin part derived from user usage of said first container **digital**information, (e) communication mean for communicatinginformation at least in part derived from user usage of saidsecond container **digital** information, (f) processing mean at aclearinghouse site for receiving the information communicatedthrough steps (d) and (e), wherein said processing means performadmini trative... ...analysis characterized bythe steps of (a) enabling plural independent clearinghouses for1083administrating and/or analyzing usage of distributed, at least inpart protected, **digital** information, (b) providing interoperableprotected processing environments to plural, independent users,and (c) enabling a user to select a clearinghouse for use with aninteroperable... ...environment497. A system for clearinghouse analysis including (a)plural independent clearinghouses for administrating and/oranalyzing usage of distributed, at least in part protected, **digital**information, (b) at least one interoperable protected processingenvironments at each of plural user locations, (c) selecting meansfor enabling a user to select one... ...independentclearinghouse to perform payment and/or analysis functionsrelated to the use of at least a portion of said at least in partprotected, **digital** information.498. A method of **electronic** advertising characterized bythe steps ofcreating one or more **electronic** advertisements, creatingone or more secure containers including at least a portion of suchadvertisements,associating control information with such advertisementsincluding control information describing... ...one or more users,enabling such users to use such containers at least in partin accordance with such control information.499. A system for **electronic** advertising including (a)means to provide **digital** information to users for their use, (b)means to provide advertising content to said users incombination with said **digital** information, (c) means to audit useof said **digital** information, (d) mean to acquire usageinformation regarding use of advertising content, (e) mean tosecurely report information based upon said advertising contentusage information... ...use of such advertisingcontent.1085. A system for chain of handling and control including(a) a first container contilinin at least in part protected **digital**information, (b) at least in part protected control informationstipulated by a first party establishing condition for use of atleast a portion of said **digital** content, (c) a second containerdifferent from said first container, said second containercontaining said first container, and (d) control informationstipulated independently by a... ...information, performing and/or causing to beperformed transactions resulting in payments to such partiesbased at least in part on such determinations.502. An **electronic** clearinghouse comprising:means for receiving usage information related at least inpart to use of secure containers from plural parties,means for determining payments due... ...the steps of receiving permissions and/or other controlinformation from one or more content providers includinginformation that enables delivery of at least one **right** in at leastone secure container to other parties, receiving requests fromplural parties for one or more **rights** in one or more securecontainers, delivering permissions and/or other controlinformation to such parties based at least in part on suchrequests.505... ...a clearinghouse characterizedby the steps of receiving information from one or more parties1087establishing a party's identity information, creating one or more**electronic** representations of at least a portion of such

identityinformation for use in enabling and/or withholding at least one**right** in at least one secure container, performing an operation tocertify such **electronic** representations, delivering such **electronic**representations to such party.506. A method of operating a clearinghouse characterizedby the steps of receiving a request for credit from a party for... ...be pefformed at least onetransaction associated with collecting payment from such user.507. A method for contributing secure control informationwith respect to an **electronic** value chain wherein controlinformation is contributed by a party not directly participating insaid value chain, comprising steps of: aggregating saidcontributed control information with control informationassociated with **digital** information stipulated by one or moreparties in an **electronic** value chain, said aggregate controlinformation at least in part managing conditions related to theuse of at least a portion of said **digital** information.1088. A method for entering the payment of taxesassociated with commercial events wherein secure controlinformation for automatically governing tax payments for said... ...aggregating said secure control information with controlinformation that has been contributed by a separate party andcontrolling at least one condition for use of **digital** information.509. A method for general purpose reusable **electronic**commerce arrangement characterized by the steps Of.(a) providing component structures, modular methods thatcan be configured together to comprise event controlled(b) providing integrateable protected processingenvironments to plural independent users;W employing secure communications means forcommunicating **digital** control information between integrateableprotected processing environments; and(d) enabling database managers operably connected tosaid processing environments for storing at least a portion of Saidprovided component modular methods.510. A system for general purpose, reusable **electronic**commerce including:(a) component modular methods configured together tocomprise event control structures;1089(b) at least one interoperable processing environment ateach of plural independent user locations;(c) secure communications means for communicating**digital** control information between interoperable protectedprocessing environments; and(d) secured database managers operably connected to saidprotected processing environments for storing at least a portionof said component modular methods.511. A general purpose **electronic** commerce credit systemincluding:(a) a secure interoperable protected processingenvironment;(b) general purpose credit control information forproviding credit for user usage of at least in part protected **digital**information; andW at least in part protected **digital** information relatedcontrol information for providing necessary information foremploying credit through the use, at least in part, of said generalpurpose credit control information.512. A method for enabling a general purpose **electronic**commerce credit system including:(a) providing secure interoperable protected processingenvironments;1090(b) supplying general purpose credit control informationfor providing credit for user usage of at least in part protected**digital** information; and(c) providing, at least in part, protected **digital** informationrelated control information for providing necessary informationfor employing credit through the use, at least in part, of saidgeneral purpose credit control information.513. A document management system comprising one ormore **electronic** appliances containing one or more SPUs and oneor more secure databases operatively connected to at least one ofthe SPUs.514. An **electronic** contract system comprising one or more**electronic** appliances containing one or more SPUs and one ormore secure databases operatively connected to at least one ofthe SPUs.515. An **electronic** appliance

containing at least one SPUand at least one secure database operatively connected to at leastone of the SPU(s).516. An **electronic** appliance containing one or more CPUswhere at least one of the CPUs is integrated with at least oneSPU.1091. An **electronic** appliance contaiinin one or more videocontrollers where at least one of the video controllers isintegrated with at least one SPU.518. An **electronic** appliance containing one or morenetwork communications mean where at least one of thenetwork communications means is integrated with at least oneSPU,519. An **electronic** appliance contstinin one or moremodems where at least one of the modems is integrated with atleast one SPU. 520. An **electronic** appliance containing one or more CD.ROM devices where at least one of the CD-ROM devices isintegrated with at least one SPU. 521. An **electronic** appliance containing one or more settop controllers where at least one of the set-top controllers isintegrated with at least one SPU.522. An **electronic** appliance containing one or more gamesystems where at least one of the game systems is integratedwiffi at least one SPU.1092. An integrated... ...software.525. An integrated circuit comprising at least onemicroprocessor, memory, input/output means, a tamper resistantbarrier and at least a portion of a **Rights** Operating System.526. An integrated circuit comprising at least onemicroprocessor, memory, input/output means, at least one realtime clock, a tamper resistant barrier...

?